Islamic University of Gaza
Deanery of Higher Studies
Faculty of Engineering
Computer Engineering Department

A Scalable Trust Management scheme For Mobile Ad Hoc Networks

By

Yaser Ali khattab

Supervisor

Prof. Mohammad A. Mikki

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering.

1434H (2013)

DEDICATION

To my great father and my great mother

To my wife and my daughter

To my dear son Ammar

And to my beautiful country "Palestine"

ACKNOWLEDGMENT

First of all, all praises be to Allah for helping me to finish this work.

I would like to record my gratitude to Prof. Mohammad Mikki for his supervision, advice, and guidance from the very early stage of this research as well as giving me extraordinary experiences throughout the work. He provided unflinching encouragement and support in various ways.

Lastly, the deepest thanks are due to my family members who have been a pillar of support during the arduous times of my research.

TABLE OF CONTENTS

List of Figuers

Abstract

A Scalable Trust Management scheme For Mobile Ad hoc Networks (MANETs)

Mobile ad hoc networks MANETs, have special resource requirements and different topology features, they establish themselves on fly without reliance on centralized or specialized entities such as base stations. All the nodes must cooperate with each other in order to send packets, forwarding packets, responding to routing messages, sending recommendations, among others, Cooperating nodes must trust each other.

In MANETs, an untrustworthy node can wreak considerable damage and adversely affect the quality and reliability of data. Therefore, analyzing the trust level of a node has a positive influence on the confidence with which an entity conducts transactions with that node.

This thesis presents a new trust management scheme to assign trust levels for spaces or nodes in ad hoc networks. The scheme emulates the human model which depends on the previous individual experience and on the intercession or recommendation of other spaces in the same radio range. The trust level considers the recommendation of trustworthy neighbors and their own experience. For the recommendation computation, we take into account not only the trust level, but also its accuracy and the relationship maturity. The relationship rationality -maturity-, allows nodes to improve the efficiency of the proposed model for mobile scenarios.

We also introduce the Contribution Exchange Protocol (CEP) which allows nodes to exchange Intercessions and recommendation about their neighbors without disseminating the trust information over the entire network. Instead, nodes only need to keep and exchange trust information about nodes within the radio range. Without the need for a global trust knowledge.

Different from most related works, this scheme improves scalability by restricting nodes to keep and exchange trust information solely with direct neighbors, that is, neighbors within the radio range.

We have developed a simulator, which is specifically designed for this model, in order to evaluate and identify the main characteristics of the proposed system. Simulation results show the correctness of this model in a single-hop network. Extending the analysis to mobile multihop networks, shows the benefits of the maturity relationship concept, i.e. for how long nodes know each other, the maturity parameter can decrease the trust level error up to 50%.
The results show the effectiveness of the system and the influence of main parameters in the presence of mobility. At last, we analyze the performance of the CEP protocol and show its scalability. We show that this implementation of CEP can significantly reduce the number messages.

Chapter One

Introduction

Chapter One: Introduction

Mobile Ad hoc Networks (MANETs) had become largely used for personal use: e.g., personal area network (PAN), for short-range communication of user devices, wireless local area network (WLAN), and in-house digital network (IHDN), for video and audio data exchange, as shown in Fig. 1.1.

Fig. 1.1. In-house digital network (IHDN).

1.1 Development of Mobile Ad hoc Networks

A mobile ad hoc network (MANET) is a self-configuring wireless network in which the routers can move and organize themselves arbitrarily [25]. Although ad hoc networking was first defined by IEEE in 802.11 protocol set, the concept can be traced back to the Packet Radio Network (PRNet) projects in 1972 [26]. Because a

MANET does not rely on the infrastructure and central management like the traditional Internet-like networks, it is deemed as a promising solution to support highly decentralized or mobile applications.

A MANET is a collection of self-organizing, peer-to-peer mobile nodes with dynamic topologies and no fixed infrastructure [27,28], which form a particular class of multi-hop networks, it is composed usually of tens to hundreds of mobile nodes, which equipped with wireless communication devices. The nodes have transmission ranges of up to hundreds of meters and each individual node must be able to act both as a host, which generates user and application traffic, and as a router which carries out network control and routing protocols [29], as shown in Fig. 1.2.

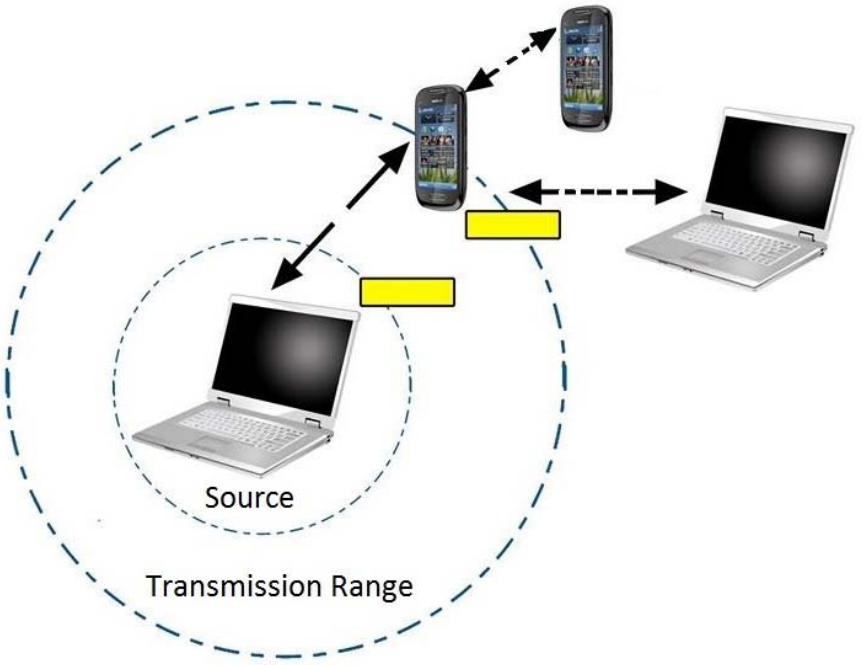


Fig. 1.2. Example: node acts as a host and as a router.

A self-configuring and self-organizing wireless network shown in Fig. 1.3, has two mechanisms implemented:

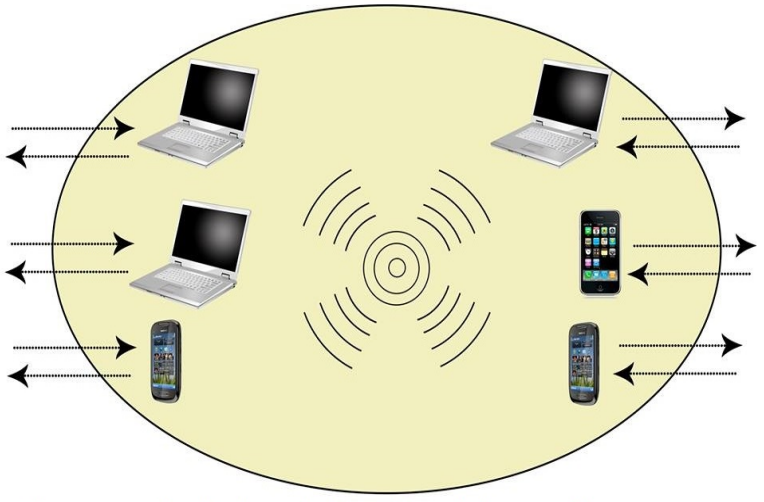
- discovery of routes between pair of nodes and,
- update the current topology, by first detecting the node or link failures and secondly by optimizing the routes obtained through discovery.
- 

Fig. 1.3. A self-configuring and self-organizing wireless network.

The discovery mechanism can be done proactively, when routes between any pairs of nodes are sought, periodically, or on-demand, when only certain routes are required. On updating the current topology, either single or multiple routes are maintained between a pair of nodes.

1.2 Routing in Mobile Ad Hoc Networks

In a MANET, nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may

change rapidly and unpredictably. In such networks, communication is achieved by forwarding packets via intermediate nodes on routes that link the source and the destination. Routes are typically determined by using on-demand routing protocols, such as the Dynamic Source Routing (DSR) [30] or the Ad hoc On-Demand Distance Vector Routing (AODV) [31], that generate routing information only when a source node initiates a transmission.

Two nodes in a MANET can communicate in a bidirectional manner if and only if the distance between them is at most the minimum of their transmission ranges. When a node wants to communicate with a node outside its transmission range, a multi-hop routing strategy is used which involves some intermediate nodes to forward their messages as shown in Fig. 1.4.

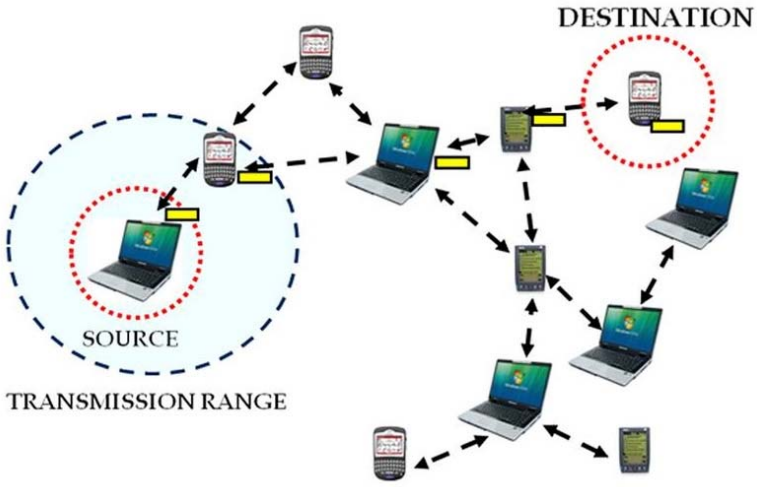


Fig. 1.4. Example: routing a message from the source to the distination.

The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae.

1.3 Broadcast in Ad Hoc Networks

Nodes in a MANET do not have a priori knowledge of the network topology. They have to discover it. A node will find its local topology by broadcasting its presence, and listening to broadcast announcements from its neighbors. As time goes on, each node gets to know about all other nodes and finds one or more ways to reach them. End-to-end communication in a MANET does not rely on any underlying static network infrastructure but requires routing via several intermediate nodes.

Nodes discover network topology using Neighbor Coverage–Based (NCB) Broadcast, nodes periodically or dynamically broadcast beacon messages to advertise their own existence and also discover the existence of neighboring nodes within the transmission range (one hop). Beacon messages may typically contain the broadcasting node's address and the neighboring nodes that the node may be aware of. Thus, the information of neighbor topology within two hops can to be obtained.

The exchange of beacon messages allows for attaching additional information about neighboring nodes. The additional information may include a node's remaining battery power, any user-based constraint, physical coordinates acquired through a GPS device, signal-to-noise

ratio (SNR) measurements (acquired from the MAC layer), and possible device characteristics such as maximum broadcast power.

The simplest NCB mechanisms are ‘‘Self-Pruning’’ [32] and ‘‘Neighbor Coverage’’ [33]. Both mechanisms are equivalent. Two neighbor sets are maintained at each node. Suppose node i broadcasts a message to node j. Set Ni and Nj denote the neighbors of node i and j, respectively. When node j receives a broadcast packet from a node i for the first time, it determines its coverage set as follows:

$$Cj = Nj \_ Ni \_ \{i\}.$$

The resulting coverage set Cj is the set of neighbors of node j, which are not covered by node i yet. This keeps track of pending hosts in j’s neighborhood, which have not received a direct broadcast from node i as they are outside node i’s broadcast range. Node j does not rebroadcast the packet if Cj is an empty set.

An empty set implies that all neighbors of node j are also neighbors of node i. This calculation is performed on each node that receives a broadcast packet prior to rebroadcasting. Nodes must share the wireless communication medium efficiently.

1.4 Mobile Ad Hoc Networks applications

Minimal configuration, Absence of infrastructure, and Quick deployment make MANETs convenient for use in situations where a network infrastructure is unavailable. For example, in some business environments, the need for collaborative computing might be more important outside the office environment than inside.

A MANET can also be used to provide crisis management services applications, such as in disaster recovery, where the entire communication infrastructure is destroyed and re-establishing communication quickly is crucial.

MANETs are attractive in military and emergency response applications, such as rapid network formation, extended operating range, and survivability. The attractiveness of these networks lies in the fact that unlike other wireless networks, ad hoc networks can establish themselves on fly without reliance on centralized or specialized entities such as base stations, and they formed dynamically in response to some immediate operational requirement.

1.5 The Problem Statement

MANETs by their very nature are more vulnerable to internal as well as external attacks than wired networks. The flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices (which have generally different resource and computational capacities, and run usually on battery power) introduces new security risks, since they obstruct the assumption of centralized or distributed online trusted authorities. Perhaps, the fundamental question that needs to be addressed in MANET is:

How to enable a mobile node to enlist trusted intermediate mobile nodes so that they can cooperate in forwarding the information to a target without modifying the information or obstructing the operation of other mobile nodes.

This advocates that the security of MANET heavily relies on the presence of a trustworthy secure communication layer so that services can be delivered at the higher layers.

Initially, several secure routing protocols [34,35] have been developed to deliver secure routes by authenticating intermediate nodes and verifying the integrity of routing messages. Data transmissions can then be protected using the secure routes discovered by these protocols. However, key management [36,37], which is the basis for proper functioning of secure routing, is difficult to achieve, especially in the absence of centralized authority due to dynamically changing topology and resulting broken links and sporadic connections. Since secure routing protocols are only designed to prevent against predefined attacks and assume all available nodes to perform routing and network management, they are prone to overlook the correct execution of critical network functions such as packet forwarding. For this reason, secure routing protocols fail to enforce cooperation among nodes .

The main reason for the shortcoming of secure routing systems is that they fail to measure the trustworthiness of nodes based on the latter's dynamically changing behavior. Therefore, a mechanism that allows a node to infer the trustworthiness of other nodes based on their behaviors becomes necessary [2,3]. All these have eventually led to the growth of trust management systems [38-43], which are synonymously referred as detection reaction and reputation systems in the literature. Since trust management systems proactively detect and

reactively isolate (or select) malicious (or benign) nodes, these systems are also known as self-policing systems [39].

1.6 WHAT IS TRUST?

Trust can be reflected by reliability, utility, availability, reputation, risk, confidence, quality of services and other concepts. Nevertheless, none of these concepts can accurately describe the definition of trust. This is because trust is an abstract concept, which combines many complicated factors [7].

Trust which is the prediction of a node's future action based on the node's past actions plays an important factor that could improve the number of successful data transmission process, by deciding from where to get a file, what service provider to contact, what access rights to grant, trust enables entities to cope with uncertainty and uncontrollability.

One of the principle problems with trust is the variety of meanings that have been associated with it. For example, in [8], Josang defines trust as a belief that one entity holds about another entity, based on past experiences, knowledge of entity behavior and/or recommendations from trusted entities. McKnight and Chervany define trust as the situation where one is willing to depend, or intends to depend, on another party with a feeling of relative security, in spite of lack of control over that party, and even though negative consequences may arise [9]. However, both these definitions predominately focus on aspects of human-mediated trust relations, it is

not immediately obvious how such a definition translates to autonomous computer networks.

Compounding this issue are the problems with the related concepts of trusted and trustworthy which are often used, but rarely clearly defined, (trustworthy; mean that there is a high probability that the actions the nodes are expected to perform will be done in a manner that is favorable to the trustor [10]), In the context of distributed systems, Anderson in [11] defines a trusted component as one whose failure can break the security policy of the system, while a trustworthy component is one that won't fail. This differs to the prevailing usage of these terms in the MANET literature in which a trusted node is one in which sufficient trust has been established, while a trustworthy node is one that will behave as expected [12]. This notion of behavior, and in particular the detection and mitigation of undesirable behavior, has received much attention in recent years [13],[12],[14].

With respect to MANET sense, trust definitions can be classified into the following:

(1) Trust as risk factor: The definition given by Morton Deutsch [15] is more widely accepted than many, and states that trusting behavior occurs when an individual (node) perceives an ambiguous path, the result of which could be good or bad, and the occurrence of the good or bad result is contingent on the actions of another person. In [16], [17] trust is defined as a bet about the future contingent actions of others.

(2) Trust as belief: Trust is an individual's belief and willingness to act on the basis of the words, actions, and decisions of another [18],[19].

(3) Trust as subjective probability: Trust (or distrust) is a particular level of subjective probability with which an agent will perform a particular action for a specified period within a specified context [20],[21]–[22].

(4) Trust as transitivity relationship: Trust is a weighted binary relation between two members of a network. As an example, consider a network of intelligence gathering agents, organized in a hierarchical manner. Trust could then be seen as the expectation of a person A (presumably high in the hierarchy) that a person B (low in the hierarchy) is honest, as opposed, being a double agent [23].

We can summarize the definition of trust in the MANETs perspective in the following way: The trust of a particular node is a subjective assessment by an agent/other peer node on the reliability and accuracy of information received from or traversing through that node in a given context. Trust reflects the belief or confidence or expectations on the honesty, integrity, ability, availability and quality of service of target node's future activity/ behavior. It also reflects the mutual relationships where a given node behaves in a trustworthy manner and maintains reliable communications only with nodes which are highly trusted by the given node.

1.7 Trust Management Systems

Trust management and trustworthy computing are becoming increasingly significant in a distributed environment, since they assist the systems in making sensible interactions with unknown parties by providing a basis for more detailed and automated decisions [43]. The concepts, trust and reputation, are closely related in trust management systems [45].

Trust system can also be used in assessing the quality of received information, to provide network security services such as access control, authentication, malicious node detections and secure resource sharing [4],[5]. An untrustworthy node can fall considerable damage and adversely affect the quality and reliability of data, therefore, it is important to periodically evaluate the trust value of nodes based on some metrics and computational methods, which has a positive influence on the confidence with which an entity conducts transactions with that node.

Providing a trust metric to each node is not only useful when nodes misbehave, but also when nodes exchange information. According to the paradigm of autonomic networks [6], a node should be capable of self-configuring, self-managing, and self-learning by means of collecting local information and exchanging information with its neighbors. Thus, it is important to communicate only with trustworthy neighbors, since communicating with misbehaving nodes can compromise the autonomy of ad hoc networks.

1.7.1 Trust and Reputation

The concepts, trust and reputation, are closely related in trust management systems [24]. Although there is no universal definition for these concepts due to their rich connection with different disciplines, we confine to computing-oriented definition. In traditional trust management systems, trust enables a trustor to reduce uncertainty in its future interactions with a trustee, who is beyond the control of trustor but whose actions are of interest to the trustor and affects the state of trustor. In other words, trust is a subjective probability that enables the trustor to take a binary decision by balancing between the known risks and the opinion held for trustee. Here, only known risks are considered for making decisions as it is difficult to prove unknown risks, and the opinion presents the trustor's relationship with the trustee based upon the trustor's experiences. Other factors that influence the decision are time and context, where context accounts for the type of interaction between trustor and trustee, and the nature of application.

A reputation system is a system that takes feedback from users and provides a mechanism to accumulate and determine the quality (or reputation) of a given source based on this feedback. In general, reputation is used to evaluate the trust of an entity. The goals of a reputation system are [46]:

- To provide information to distinguish a trustworthy principal from an untrustworthy one.
- To encourage principals to act in a trustworthy manner.

- To discourage untrustworthy principals from participating in the service that the reputation mechanism protects.

Reputation mechanisms that are applied to MANETs to address threats arising from uncooperative nodes rely on neighbor monitoring to dynamically assess the trustworthiness of neighbor nodes and exclude untrustworthy nodes.

Several reputation systems have been proposed to mitigate selfishness and stimulate cooperation in MANET, including CONFIDANT [47-49], CORE [50] and OCEAN [51].

In reputation systems, reputation is defined as the opinion held by the trustor towards the trustee depending on its past experiences with the trustee [24]. In other words, reputation generally represents the trustor's direct relationship with the trustee. Also, trustor's relationship with a second trustee based on its direct relationship with a first trustee and the first trustee's direct relationship with the second trustee is known as indirect relationship. This is possible as nodes are allowed to share their opinions in the network.

Although trust and reputation are used interchangeably in MANET, we define them as follows since they are shown to complement each other from the above discussion. Hence, trust can be defined as the prediction of a node's future action in a context such as forwarding routing messages without modification, while reputation then becomes the opinion held for the node based on the node's past actions and the one that influences the prediction. For this reason, we consider the following trust definition to be more appropriate and timely: ''Trust is the firm belief in the competence of an entity to act as expected such

that this firm belief is not a fixed value associated with the entity but rather subject to the entity's behavior (reputation held for the entity) and applies only within the context and at a given time.'' .

1.8 Trust research directions in MANETs

Trust researches are organized in four major areas:

1. Policy-based trust: Using policies to establish trust, focused on managing and exchanging credentials and enforcing access policies. Work in policy-based trust generally assumes that trust is established simply by obtaining a sufficient amount of credentials pertaining to a specific party, and applying the policies to grant that party certain access rights. The recursive problem of trusting the credentials is frequently solved by using a trusted third party to serve as an authority for issuing and verifying credentials.

2. Reputation-based trust: Using reputation to establish trust, where past interactions or performance for an entity are combined to assess its future behavior. Research in reputation-based trust uses the history of an entity's actions/behavior to compute trust, and may use referral-based trust (information from others) in the absence of (or in addition to) first-hand knowledge. In the latter case, work is being done to compute trust over social networks (a graph where vertices are people and edges denote a social relationship between people), or across paths of trust (where two parties may not have direct trust information about each other, and must rely on a third party). Recommendations are trust decisions made by other users, and combining these decisions

to synthesize a new one, often personalized, is another commonly addressed problem.

3. General models of trust: There is a wealth of research on modeling and defining trust, its prerequisites, conditions, components, and consequences. Trust models are useful for analyzing human and agentized trust decisions and for operationalizing computable models of trust. Work in modeling trust describes values or factors that play a role in computing trust, and leans more on work in psychology and sociology for a decomposition of what trust comprises. Modeling research ranges from simple access control polices (which specify who to trust to access data or resources) to analyses of competence, beliefs, risk, importance, utility, etc. These subcomponents underlying trust help our understanding of the more subtle and complex aspects of composing, capturing, and using trust in a computational setting.

4. Trust in information resources: Trust is an increasingly common theme in Web related research regarding whether Web resources and Web sites are reliable. Moreover, trust on the Web has its own range of varying uses and meanings, including capturing ratings from users about the quality of information and services they have used, how web site design influences trust on content and content providers, propagating trust over links, etc.. With the advent of the Semantic Web, new work in trust is harnessing both the potential gained from machine understanding, and addressing the problems of reliance on the content available in the web so that agents in the Semantic Web can ultimately make trust decisions autonomously. Provenance of information is key to support trust decisions, as is automated detection of opinions as distinct from objective information.

Therefore, a mechanism that allows a node to infer the trustworthiness of other nodes in an ad hoc network becomes necessary.

Providing a trust metric to each node is not only useful when nodes misbehave, but also when nodes exchange information.
According to the paradigm of autonomic networks [72], a node should be capable of self-configuring, self-managing, and self-learning by means of collecting local information and exchanging information with its neighbors. Thus, it is important to communicate only with trustworthy neighbors, since communicating with misbehaving nodes can compromise the autonomy of ad hoc networks.

1.9 Thesis Methodology and Objectives

The fundamental question that this thesis will address is:
How to enable a mobile node to enlist trusted intermediate mobile nodes so that they can cooperate in forwarding the information to a target without modifying the information or obstructing the operation of other mobile nodes.
So the objectives of this thesis will include:

1- Propose an alternative trust management model by fruitfully combine more than one idea which emulate the human trust model to improve the trustworthiness of the neighborhood and secure the routing procedure. This will help in computing the trust in the neighbors, based on previous individual experience and the intercession of the others, and then selecting the most trustworthiness route from the available ones for the data transfer (integrated security solution).

2- Introduce a light and simple Contribution Exchange Protocol (CEP) which allows nodes to exchange Intercessions about their neighbors without disseminating the trust information over the entire network.

This research introduce a flexible trust model based on the concept of human trust model, and applies this model to ad hoc networks. The trust is based on previous individual experiences and on the recommendations of others, A key concept introduced is the relationship maturity, which allows spaces to improve the efficiency of the proposed model for mobile scenarios.

The rest of the thesis report is organized as follows: chapter two presents and discusses some of the existing trust- and reputation-based schemes designed for MANETs. chapter three describes the proposed model in detail. Chapter four presents the simulation and results. Finally, Chapter five concludes the proposed model, and present the future work.

Chapter two

literature review

literature review

There have been different approaches to define trust. Trust, in general, is a directional relationship between two entities and plays a major role in building a relationship between nodes in a network. Even though trust has been formalized as a computational model, it still means different things for different research communities. For example, the problem of defining trust metrics and trust relationship has been extensively studied for public key authentication [77][78][79], electronic commerce [80], as well as in P2P networks [81]. In some of these schemes, discrete or continuous numerical values are assigned to measure the level of trust [78][79][80]. For example, in [81], an entity's opinion about the trustworthiness of a certificate is described by a continuous value in [0,1]. In [79], a triplet in [0, 1] is assigned to measure the trustworthiness where the elements in the triplet represent belief, disbelief, and uncertainty respectively. In [81], discrete integers are used. In [82] failed and selfish behaviors in ad hoc networks are studied.

The *reputation* of an entity has been defined as an expectation of its behavior based on other entities' observations or information about the entity's past behavior within a specific context at a given time [83]. In case of a MANET, the reputation of a node refers to how good the node is in terms of its contribution to routing activities in the network.

The *distributed trust model* proposed by Abdul-Rahman et al. uses a recommendation protocol to exchange trust-related information [84]. The trust relationships are assumed to be unidirectional between two

entities. The recommendation protocol works by requesting a trust value in a target node with respect to a particular classifier. When the response arrives, an evaluation function is used to compute the overall trust value in the target. The protocol also allows recommendation refreshing and revocation. The model is suited for systems that are less formal and temporary in nature, e.g., some ad hoc commercial transactions.

The *resurrecting duckling* security protocol proposed by Stajano et al. is particularly suited for devices without display and embedded devices that are too weak for public-key operations [85].

The authentication problem is solved by a secure and transient association between two devices establishing a master-slave relationship. The association is secure because the master and the slave share a common secret, and it is transient because it can be terminated by the master at any point of time.

Kong et al. have proposed a trust building scheme for ad hoc networks that is similar to the pretty good privacy (PGP) web of trust concept [96]. However, unlike PGP it has no central certificate directory. In order to find the public key of a remote user, a local user makes use of the Hunter algorithm [97] on the merged certificate repository to build certificate chain(s).

Eshenauer et al. have proposed a trust establishment mechanism for MANETs [86]. In this scheme, a node in the network can generate trust evidence about any other node. When a principal generates a piece of trust evidence, it signs the evidence with its own private key, specifying the lifetime and makes it available to other through the network. A principal node may revoke a piece of evidence it produced

by generating a revocation certificate for that piece of evidence and making it available to others, at any time before the evidence expires. A principal can get disconnected after distributing trust evidence. Similarly, a producer of trust evidence does not have to be reachable at the time its evidence is being evaluated. Evidences can be replicated across various nodes to guarantee availability. Although the scheme seems conceptually sound, the authors have provided no details about any performance evaluations.

Among the more recent works, Repantis et al. have proposed a decentralized trust management middleware for ad hoc, peer-to-peer networks based on reputation of the nodes [87]. In this scheme, the reputation information of each peer is stored in its neighborhood and piggybacked on its replies.

In the trust-based data management scheme proposed by Patwardhan et al., mobile nodes access distributed information, storage and sensory resources available in pervasive computing environment [88]. The authors have taken a holistic approach that considers data, trust, security, and privacy issues and utilizes a collaborative mechanism that provides trustworthy data management platform in a MANET.

Sun et al have presented a framework to quantitatively measure trust, model trust propagation, and defend trust evaluation system against malicious attacks [39]. The attacks against trust evaluation are identified and defense techniques have been proposed.

Baras and Jiang have presented a trust management scheme for self-organized ad hoc networks, where the nodes share trust information only with their neighbors [93]. For establishing and maintaining trust among the neighbors, the authors have proposed a voting mechanism.

Chang et al. have proposed a trust-based scheme for multicast communication in a MANET [91]. In a multicast MANET, a sender node sends packets to several receiving nodes in a multicast session. Since the membership in a multicast group changes frequently in a MANET, the issues of supporting secure authentication and authorization in a multicast MANET is very critical. The proposed scheme involves a two-step secure authentication method. First, an ergodic continuous Markov chain is used to determine the trust value of each one-hop neighbor. Second, a node with the highest trust value is selected as the certificate authority (CA) server. For the sake of reliability, the node with the second highest trust value is selected as the backup CA server. The analytical trust value of each mobile node is found to be very close to that observed in the simulation under various scenarios. The speed of the convergence of the analytical trust value shows that the analytical results are independent of the initial values and the trust classes.

Sun et al. have presented trust as a measure of uncertainty [92]. Using the theory of entropy, the authors have developed a few techniques to compute trust values from certain observations. In addition, trust models – entropy-based and probability-based, presented to solve the concatenation and multi-path trust propagation problems in a MANET.

Sen et al. have proposed a self-organized trust establishment scheme for nodes in a large-scale MANET in which a trust initiator is introduced during the network bootstrapping phase [93]. It has been proven theoretically and shown by simulation that the new nodes joining the network have high probability of successful authentication

even when a large proportion of the existing nodes leave the network at any instant of time. A distributed intrusion detection system has been proposed in [94], where local anomaly detection is utilized to make a more accurate networkwide (i.e. global) detection using a cooperation detection algorithm among the nodes.

Cooperation Of Nodes-Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT) is a security model based on selective altruism and utilitarianism proposed by Buchegger and Boudec to make misbehaviour unattractive in MANETs [95]. It is a distributed, symmetric reputation model that uses both first-hand and second-hand information for computation of reputation values. CONFIDANT uses dynamic source routing (DSR) protocol for routing and assumes that promiscuous mode of operation is possible. The misbehaving nodes are punished by isolating them from accessing the network resources.

Although researchers usually assume that nodes collaborate in ad hoc networks, it is not so obvious that this collaboration exists in practical networks. Each node must forward packets for other nodes and spend its energy without receiving any direct gain for this act. There is no real incentive for nodes to participate in the routing and forwarding process. Yu and Liu [52] state that before ad hoc networks can be successfully deployed in autonomous ways, the issues of cooperation stimulation and security must be resolved first. Several works propose mechanisms to stimulate the cooperation among nodes. Their goal is to avoid selfish and malicious behavior to guarantee the right implementation of routing and forwarding tasks by all nodes of the network [53-59]. Nevertheless, all these works are restricted to stimulate the collaboration of nodes to relay traffic for other nodes.

We are concerned with all kinds of distributed mechanisms and applications, such as authentication, key distribution, access control, and management.

In general, the trust models in ad hoc networks try to protect or enforce the two basic functions of the network layer: routing and packet forwarding [60]. Sun et al. [61] investigate the benefits of using trust models in distributed networks, the vulnerabilities in trust establishment methods, and the defense mechanisms.

Several works propose monitoring schemes to generate trust values describing the trustworthiness, reliability, or competence of individual nodes. Theodora kopoulos and Baras [62] analyze the issue of evaluating the trust level as a generalization of the shortest-path problem in an oriented graph, where the edges correspond to the opinion that a node has about other node. They consider that nodes use just their own information to establish their opinions. The opinion of each node includes the trust level and its precision. The main goal is to enable nodes to indirectly build trust relationships using exclusively monitored information.

Sun et al. [63] have developed a framework capable of measuring the trust level and propagating it through the network in order to make routing more secure and to assist intrusion detection systems. The framework includes a defense mechanism against malicious nodes. The authors use a probabilistic model based on the uncertainty of a neighbor to execute one specific action and consider only the monitoring information.

He et al. [64] propose an architecture for stimulating the collaboration based on the reputation of nodes. The system is based only on the

monitored information to evaluate the reputation of nodes. The goal is to detect and to punish nodes that do not participate in the routing process.

The main difference of these works and our trust model is that they use only the node own experience, namely, the monitored information on the trust evaluation process. Our trust model considers the monitored information and the recommendations of neighbors to achieve a faster convergence time and an accurate trust level for each neighbor.

In probabilistic-based models, a common approach consists of using Bayesian networks, which is a probabilistic tool that provides a flexible means of dealing with probabilistic problems involving causality [65]. Buchegger and Le Boudec [66] investigate the trade-off between robustness and efficiency of reputation systems in mobile ad hoc networks. A mechanism based on Bayesian statistics is used to filter slanderer nodes.

The proposed system considers the monitored information and the recommendation of other nodes to compute the reputation of a specific node. They show that taking into account the recommendations of other nodes can speed up the process of discovery of malicious nodes.

Chinni et al. [67] offer a distributed trust model for certificate revocation in ad hoc networks. This model allows trust to be built based on the interactions between nodes, using monitored information. Furthermore, trust in a node is defined not only in terms of its potential for maliciousness, but also in terms of the quality of the service it provides. The trust level of nodes where there is little or no history of interactions is determined by recommendations from other

nodes. If the nodes in the network are selfish, trust is obtained by an exchange of portfolios. Bayesian networks form the underlying basis for this model.

Another approach consists of using linear functions to infer trust. Pirzada and McDonald [68] propose another trust model for ad hoc networks to compute the trustworthiness of different routes. Nodes can use this information as an additional metric on routing algorithms. Although the authors present an interesting approach, the model presents 1 relies on using the promiscuous mode, ignoring the energy constraints of mobile nodes. Finally, it requires each node to store information for all other nodes in the network, which is not scalable.

Liu et al. [73] propose a trust model to ad hoc networks based on the distribution of threat reports to interested nodes. The goal is to make security-aware routing decisions, where nodes use the trust level as an additional metric for routing packets. The authors present different approaches for the trust level calculation. Nevertheless, they assume that nodes cooperate with each other which is not always the case. They also assume that all nodes are capable of detecting malicious behavior by means of Intrusion Detection Systems (IDS). This assumption leads to high energy consumption, which is clearly not an appropriate option for ad hoc networks. All the trust level dynamics is based on the reports provided by the IDS.

Yan et al. [74, 75] propose a security solution for ad hoc networks based on a trust model. They suggest using a linear function to calculate the trust according to a particular action. The function considers different factors that can affect the trust level, including intrusion black lists, previous experience statistics, and

recommendations. Nonetheless, the influence of such factors on the trust evaluation is not defined. Although mentioning general trust concepts, the work focus on specific routing issues.

Pirzada and McDonald [76] propose another trust model for ad hoc networks to compute the reliability of different routes. Nodes can use this information as an additional metric on routing algorithms. The authors propose an extension to DSR protocol which applies their trust model in order to find trustworthy routes. Although the authors present an interesting approach, the model presents several disadvantages. For instance, it is restricted to DSR so far, it relies on using promiscuous mode ignoring the energy constrains of mobile nodes, and it stores a significant amount of information, since it keeps information for all nodes in the network.

Virendra et al. [71] present a trust-based architecture that allows nodes to make decisions on establishing keys with other nodes and forming groups of trust. Their scheme considers trust self-evaluation and recommendation of other nodes to compute trust. Their trust self-evaluation is based on monitoring nodes and a challenge-response system. Some authors present trust models specifically designed to work with a particular routing protocol. Komathy and Narayanasamy [69] add a trust-based evolutionary game model to the AODV routing protocol in order to cope with selfish nodes.

Kostoulas et al. [71] propose a decentralized trust model to improve reliable information dissemination in large-scale disasters. The proposed model includes a distributed recommendation scheme, incorporated into an existing membership maintenance service for ad

hoc networks. In addition, trust based information is propagated through a nature-inspired activation spreading mechanism.

The main differences of our work from all the related work are that nodes interact only with neighbors. Neighborhood interactions imply low resource consumption and minimize the effect of false recommendations. Another important issue is the introduction of the concept of relationship maturity in our model which improves the efficiency of the trust model in MANETS.

Chapter Three

A Scalable Trust Management scheme For Mobile Ad Hoc Networks

A Scalable Trust Management scheme for MANETs

Mobile ad hoc networks MANETs, lack the infrastructure seen in managed wireless networks. As a result, nodes must play the roles of router, server, and client, compelling them to cooperate for the correct operation of the network [1]. Specific protocols have been proposed for ad hoc networks considering not only its peculiar characteristics, but also a perfect cooperation among nodes. In general, it is assumed that all nodes behave according to the application and protocol specifications. This assumption, however, may be false, due to resource restrictions (e.g., low battery power) or malicious behavior. Assuming a perfect behavior can lead to unforeseen pitfalls, such as low network efficiency, high resource consumption, and vulnerability to attacks. Therefore, a mechanism that allows a node to infer the trustworthiness of other nodes in an ad hoc network becomes necessary [2],[3].

Providing a trust metric to each node is not only useful when nodes misbehave, but also when nodes exchange information.

According to the paradigm of autonomic networks [72], a node should be capable of self-configuring, self-managing, and self-learning by means of collecting local information and exchanging information with its neighbors. Thus, it is important to communicate only with trustworthy neighbors, since communicating with misbehaving nodes can compromise the autonomy of ad hoc networks.

The ability of assessing the trust level of a neighbors brings several advantages:

First: A node can detect and isolate malicious behaviors, avoiding relaying packets to malicious neighbors.
Secondly: cooperation is stimulated by selecting the neighbors with higher trust levels.

This flexible trust model is based on the concept of human trust principles, which consider the previous individual experiences (judging the actions performed by other nodes) and on the recommendations of others (experiences of other nodes), a key concept introduced is the relationship maturity, which is the age of the relationship between two nodes. This concept allows nodes to give more importance to recommendations sent by long-term neighbors than recommendations sent by new neighbors. Hence improve the efficiency of the proposed model for mobile scenarios.

3.1 THE TRUST MODEL

The basic idea is to build a trust model that provides nodes with a mechanism to evaluate the trust of its neighbors. A node assigns a so-called trust level for each neighbor, which represents how trustworthy each neighbor is. In this work trust is defined as the value that reflects the behavior history that a node has about a specific neighbor. This information is used as an expectation of its neighbor future behavior. We extend this definition to include the recommendations of others as well. Therefore, similar to the concept of human trust, the computation of the trust level of a given neighbor is based on previous experiences and also on the opinion of other neighbors.

By previous experiences, we mean that a node keeps track of the good and bad actions taken by its neighbors. A bad action is the one that does not correspond to the expected behavior. As a result, previous experiences allow a node to have a personal "opinion" about all its neighbors.

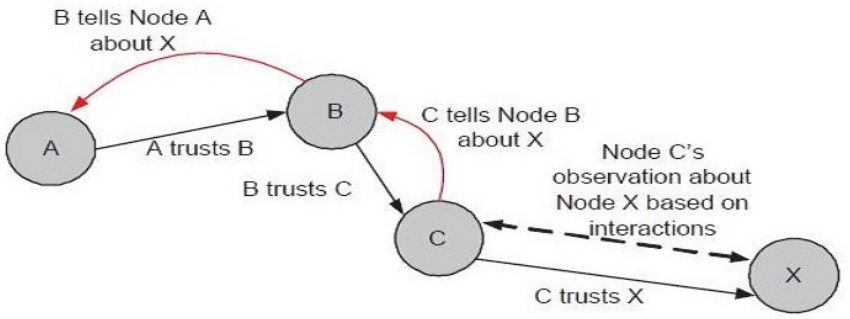


Fig. 3.1. Propagation of trust in a simple straight chain.

Neighbor nodes can further share their own opinions in order to improve the trust level evaluation, as shown in figure 3.1. The transmission of a personal opinion about a specific node i is defined as a recommendation. Neighbor nodes take into account this recommendation while calculating the trust level for node i. The main goal of the recommendations is to compensate for the lack of monitoring capabilities due to resource constraints.

Usually, a node is not able to observe the complete behavior of a given neighbor over time. Recommendations from other neighbors are useful in this case for an accurate trust level assignment. Moreover, the use of recommendations can speed up the convergence of the trust evaluating process, as showed in chapter four. For that purpose, we introduce the concept of relationship maturity, which is based on the age of the relationship between two nodes. This concept allows nodes

to give more importance to recommendations sent by longterm neighbors rather than short-term neighbors. Nodes use the Contribution Exchange Protocol (CEP) to send and receive recommendations. Figure 3.2. illustrates an example of a recommendation. Nodes connected by a dotted arrow are neighbors

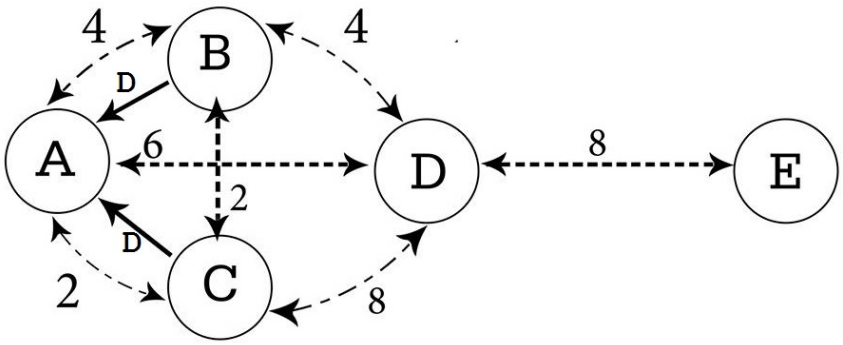


Fig. 3.2. Node *A* receive recommendations about node *D*.

and the number indicates for how long they know each other, namely, the relationship maturity parameter. A normal arrow represents a recommendation and the letter indicates the target node.

First thing to notice is that recommendations concern one common neighbor of different nodes. In that case, node D is a common neighbor of node A, B, and C. Node B and C send their recommendation about node D to node A. Node A will consider the recommendation from node C more important than the one received from node B because node C has a longer relationship with node D. It is worth mentioning that recommendations sent by node D about node E will be ignored by node A, B, and C because node E is not a neighbor of A. Each node assigns a trust level for each neighbor. A continuous representation for the trust level is maintained, ranging

from 0 to 1 where 0 means the least reliable node and 1 means the most reliable node.

The proposed model can be divided in two distinct planes as shown in Fig. 3.3.

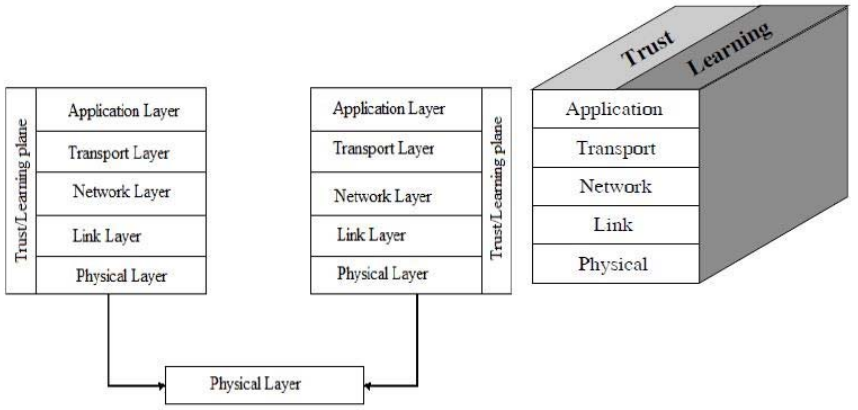


Fig. 3.3. The proposed trust model architecture.

The Learning plane is responsible for gathering and converting information into knowledge. For instance, this plan is responsible for monitoring the behavior of each neighbor. The Trust plane defines how to assess the trust level of each neighbor using the knowledge information provided by the Learning plan and the information exchanged with neighbors. Both plans can interact with all layers of the TCP/IP model. Therefore, the learning process considers information from all layers and the trust information generated by the Trust plane is also available for all layers. Since we take into account not only malicious nodes but also selfish behaviors due to resource constraints, a trust value is associated to a particular scope, like forwarding packets, sending recommendations, and other application-specific scopes.

Therefore, we consider that a node might behave differently according to the scope and the resource constraints. Consequently, the type of information to be collected by the Learning plan depends on the defined scopes. For instance, for the routing process, the Learning plan must observe if neighbors respond to route requests, if they send false routes, etc.

The Learning plan relies on three basic components as displayed in Fig. 3.4. The Behavior Monitor observes neighbors in order to collect information about their behavior. It must be able to notice other nodes' actions and transmit them to the Classifier. In ad hoc networks, nodes might perform several actions, like sending packets, forwarding packets, responding to routing messages, among others. For this, each node periodically broadcasts its hello messages, containing the list of neighbors known to the node and their link status. The hello messages are received by all one-hop neighbors, but are not forwarded. They are broadcast at a low frequency determined by the refreshing period Hello Interval (the default value is two seconds). These hello messages permit each node to absorb the knowledge of its neighbors up to two hops. On the basis of this information, each node performs the selection of its multipoint relays.

The Behavior Monitor also indicates the presence of new neighbors to the Recommendation Manager. The Classifier is the component dedicated to reason about the information collected by the Monitor. The Classifier decides the quality of an action according to a previously defined classification. The Classifier then sends its verdict to the Experience Calculator. Finally, the Experience Calculator

estimates a partial trust value for a given node based on the information received by the Classifier.

The trust plan is composed of five main components as depicted in Fig. 3.4.

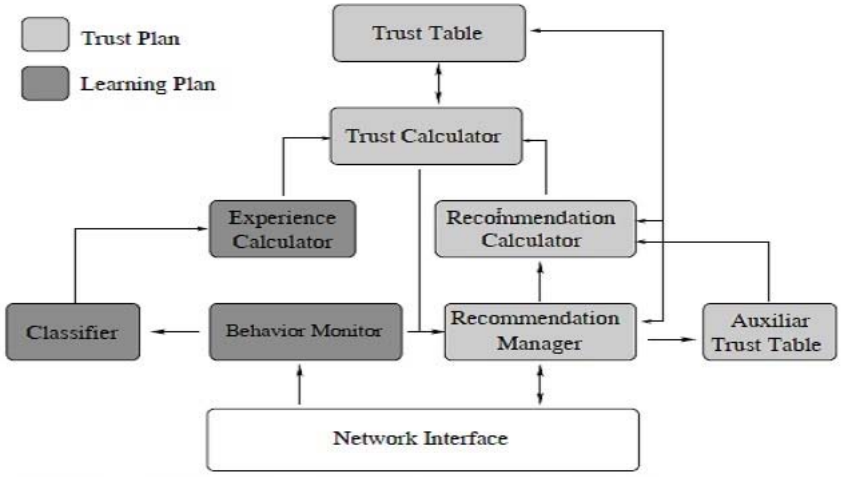


Fig. 3.4. The proposed trust model component.

Each node must keep a main Trust Table which contains the trust level for each neighbor. Additionally, a node can also store the opinion of its neighbors about their common neighbors on the Trust Table. Each entry on the Trust Table is associated with a timeout. Therefore, an entry is erased from the Trust Table whenever the node associated to that entry is no longer a neighbor or when it expires. All the recommendations related to that entry are erased as well. In our model, nodes can also keep an additional table that is not mandatory. The Auxiliary Trust Table (ATT) contains the variance of each trust level and for how long they keep that information, which indicates relationship maturity. The goal of the Auxiliary Trust Table is to supply nodes with additional information that improves the trust level

evaluation. Nevertheless, this trust evaluation improvement requires more energy consumption and nodes with power or storage constraints can choose not to implement the entire trust system. Thus, in order to cope with the heterogeneity that characterizes ad hoc networks [12], we define three operation modes: simple, intermediate, and advanced:

- Nodes with low power/storage capacity operate in the simple mode, in which they use just the main Trust Table.

- Nodes with a medium capacity operate in the intermediate mode, in which they use the main trust table and also store the trust table of neighbor nodes.

- Nodes with high capacity operate in the advanced mode, which is the same as intermediate mode, but additionally implement the ATT to keep track of additional parameters, like maturity, accuracy, and location.

The amount of saved resource and the accuracy of trust level for each operation mode depends on the monitoring, which is application-specific, and whether the CEP protocol is used or not. we consider that nodes operate in the advanced mode.

The Recommendation Manager is responsible for receiving, sending, and storing recommendations. The interactions between the Network Interface and the Recommendation Manager are performed by the Contribution Exchange Protocol (CEP). The reception of a recommendation involves two actions. First, the recommendation is stored in the Auxiliary Trust Table (ATT) and then it is forwarded to the Recommendation Calculator component. The Recommendation

Calculator computes all the recommendations for a given neighbor and determines a trust value based on the opinions of other nodes. This value is passed to the Trust Calculator component.

The Trust Calculator evaluates the trust level based on the trust values received from the Experience Calculator (individual experiences) and the Recommendation Calculator (neighbor recommendations). The Trust Calculator also notifies the Recommendation Manager the need of sending a trust recommendation advertisement. Our proposition only requires interactions with neighbors and only stores information about neighbors. This is an important feature for mobile ad hoc networks composed by portable devices that have energy, processing, and memory restrictions [13]

3.2 Trust level evaluation

We define the trust level evaluation from node a about node b, $Ta(b)$, as a weighted sum of its own trust (monitor) and the recommendations of neighbors, similar to Virendra *et al.* [14]. The fundamental equation is:

$$T_a(b) = (1-\alpha)\, Q_a(b) + \alpha\, R_a(b), \qquad (1)$$

where the variable Qa(b), that ranges from [0,1], represents the capability of a node a to evaluate the trust level of its neighbor b based on its own information (observations). and Ra(b) that ranges from [0,1], is the aggregate value of the recommendations from all other neighbors, explained in Section 3.3. The variable α that ranges from [0, 1], is a parameter that allows nodes to choose the most relevant factor. The value of Qa(b) is given by:

$$Q_a(b) = \beta E_a(b) + (1 - \beta) T_a(b), \qquad (2)$$

where E_a represents the trust value obtained by the judgment of the actions of a neighbor performed by the Classifier component, and the variable Ta(b) gives the last trust level value stored in the Trust Table. The variable β, that ranges from [0, 1], allows different weights for the factors of the equation, selecting which factor is the more relevant at a given moment.

Equations 1 and 2 describe how the Trust Calculator combines the information from the Experience Calculator (Ea(b)), the Recommendation Calculator (Ra(b)), and the Trust Table (Ta(b)) to derive a trust level.

3.3 Recommendation computation

The trust level calculation considers the recommendations of neighbors obtained by the Contribution Exchange Protocol (CEP) described in Section 3.5. Ra(b), in Equation 1, represents the aggregate trust that the neighbors of node a have on node b.

First, node a defines a set *Ka,* the group *Ka* defines the nodes from which recommendations will be considered. Let *Na* be the set of neighbors of node a that includes all nodes known for a period of time. *Ka* is a subset of the neighbors of node a comprising all nodes that satisfy two basic conditions :

- Theire trust level is above a certain threshold *(Tth).*
- Theire relationship maturity factor are above certain threshold *(Mth).*

The subset *Ka* can be defined as follows:

$$Ka = \{ \forall_i \in Na \mid Ta(i) \geq Tth \cap Ma(i) \geq Mth \}.$$

The recommendation, $Ra(b)$, is defined as the weighted average of the recommendations from all nodes $i \in K_a$ about node b. The weight for a recommendation from a neighbor i is the trust level that node a has on node i, $Ta(i)$, as follows:

$$Ra(b) = \frac{\sum_{i \in k_a} Ta(i)\, Mi(b)\, Xi(b)}{\sum_{j \in k_a} Ta(j)\, Mj(b)}, \qquad (3)$$

The relevance of the recommendation of other nodes is strongly related to the selection of *Ka*. The more trustworthy *Ka* is the more useful the recommendation of others is. The recommendations considers not only the trust level of other nodes $Ti(b)$, but also the accuracy (X_i) and the relationship maturity (M_i). The accuracy of a trust level is based on the standard deviation, similar to Theodorakopoulos and Baras [15]. The value in the Trust Table of node i regarding node b is associated to a standard deviation $\sigma_i(b)$, which refers to the variations of the trust level that node i has observed about node b. We use X as a random variable with a normal distribution to represent the uncertainty of the recommendation. It can be expressed as:

$$Xi(b) = N(Ti(b), \sigma i(b)). \qquad (4)$$

The vaule of $\sigma_i(b)$ is defined as

$$\sigma i(b) = \sqrt{\frac{\sum_{j=1}^{k} (\bar{S} - s_j)^2}{K-1}} \qquad (5)$$

where S represents the set of the k last trust level samples about a specific node. The value of $\bar{S}$ represents the average of these k samples. The parameter $\sigma i(b)$ tells us the confidence of the trust level. A high value fot $\sigma i(b)$ has two meanings:

- Either the node is not able to assess the trust value with accuracy or,
- The node whose trust level is being estimated is unstable.

The recommendation of node (i) about node (b) is weighted by $M_{i(b)}$, which defines the maturity of the relationship between nodes i and b, measured at node(i). The relationship maturity is a measure of the time that two nodes have known each other. We use the relationship maturity to give more relevance to the nodes that know the evaluated neighbor for a longer time. Accordingly, we assume that the trust level of a more mature neighbor (older neighbor) has already converged to a common value within the network and therefore its opinion should be more relevant than the opinion of a new neighbor. It is important to notice that maturity is only considered between the recommender, node (i), and the node that is being evaluated, node (b), as illustrated in Fig. 7.

Malicious nodes can implement an attack exploiting the concept of relationship maturity by attributing fake trust levels. In order to minimize this effect, each node defines a maximum relationship maturity value M_{max}, which represents an upper bound for the relationship maturity. This value is based on the average time for

which a node knows its neighbors.Accordingly, we can express *Mi*(*b*) as:

$$M_i(b) = M_{max}, \text{ if } Mi(b) >= M_{max}, \text{ Else, } Mi(b).$$

3.4 The First Trust Assignment

We divide the trust scheme in two distinct phases. In the initial phase, nodes first meet and assign a trust level to each other. The second phase is the trust level update, which assumes that the nodes have already met each other. When a node first meets a specific neighbor, it assigns an initial level of trust to this neighbor. The first trust assignment depends on several network parameters, such as mobility, location of nodes, and its current state. We classify the first trust assignment strategy as prudent or optimistic. In the prudent strategy the node does not trust strangers and considers that every new neighbor as a possible threat to the network. As a consequence, the node assigns a low value of trust for the new neighbor. On the other hand, the optimistic strategy assumes that every node is reliable until proven otherwise. In such case, the node associates a high level of trust for new neighbors. Right in the middle of these two strategies, one could think of a moderate strategy, in which the node assigns an intermediate level of trust for strangers.

Different situations might demand distinct strategies. For example, if a has already a significant number of reliable neighbors it can adopt a prudent strategy because it does not need new reliable neighbors. Further, the addition of a new neighbor might not significantly increase the probability of augmenting its satisfaction level. On the other hand, in a network where topology periodically changes and

neighbor relationships are ephemeral, a node can opt for the optimistic strategy. In hostile environments, nodes might want to adopt the prudent strategy whereas in well-known cordial environments nodes can select the friendly strategy.

The first trust assignment can also take into account the recommendation of known neighbors weighted by their trust levels. For a node a to calculate the first trust level of a node b, we propose the same approach as Equation 1, but replacing the term that reflects its own experience by the First Trust Value, (F_a), given by:

$$T_a(b) = (1-\alpha)F_a + \alpha R_a(b), \qquad (6)$$

where F_a is the value used by node a according to the adopted strategy, $Ra(b)$ is the aggregate recommendation of neighbors about node b, and α is the weight factor that allows us to give more relevance to the desired parameter.

3.5 The Contribution Exchange Protocol

The recommendation from node $i \in k_a$ includes the trust level $T_{i(b)}$ of the target node, its accuracy $\sigma_{i(b)}$ and for how long they know each other, $M_{i(b)}$. For a node that does not implement the Auxiliary Trust Table, the recommendation includes just the trust level $T_{i(b)}$. We propose the Contribution Exchange Protocol (CEP) as a part of the Recommender Manager in Fig. 3.4. This protocol allows nodes to exchange recommendations among them and only considers interactions with neighbors, which significantly simplifies the protocol. Thus, all messages are transmitted by one hop broadcasts

avoiding flooding in multihop communications. When using IP to broadcast the message, the Time to Live (TTL) field is set to 1.

The protocol is composed of three messages:

- Trust Request (T_{REQ}) message.
- Trust Reply (T_{REP}) message.
- Trust Advertisement (T_A) message.

When nodes first meet, each one broadcasts a Trust Request (T_{REQ}) message to their neighbors with the IP address of the new neighbor as the target node. All neighbors receive the (T_{REQ}) message and check if the target node is a neighbor or not. Nodes that have the target node as a neighbor, will answer with a Trust Reply (T_{REP}) message, which contains the recommendation about the target node, after waiting for a random period of time t_{REP} to avoid collisions and to wait for receiving other (T_{REQs}).

Trust Level Assignment Pseudocode

Start
New nodes meet
Wait t_{REQ} *time*
For each node $N \in k_a$ *node's neighbors*
Begin
    Broadcast a Trust Request (newNodeIP)
    If newNode in N's neighbors
    Begin
        Wait t_{REP} *random time(To avoid collisions and to wait for receiving other TREQs)*
        Send T_{REP} *as a recommendation with newNode* T_L.
    End
End
Wait specific time

IF no receiving of T_{REP}
Begin
Alfa=0
End
If the trust level changes.
Begin
For each node N∈ k_a node's neighbors
Begin
Send T_A
End
End
End

We also define a T_{REP} threshold under which it will not answer the T_{REQ}. The threshold is based on the trust level of the requesting node. This strategy reduces the effect of non trustworthy nodes that repeatedly send T_{REQ} messages. Before sending a T_{REQ} message, a node waits for a specific period of time t_{REQ} trying to gather the maximum number of new neighbors. After t_{REQ}, the node will request the recommendations of all the q new neighbors it has collected. Thus, instead of sending q T_{REQ} messages it sends just one with q node ID_s. After sending a T_{REQ}, the trust requesting node will wait for a specific timeout period to receive the T_{REPs} from its neighbors. If a node does not receive any T_{REP}, it ignores the recommendation of its neighbors by choosing $\alpha = 0$ in Equation 5.

During a trust level update, the Trust Level (T_L) may change. If the trust level changes significantly, the node sends a Trust Advertisement (T_A) message to notify its neighbors about the change. In order to prevent nodes from sending T_A messages for every change in the Trust Level, we defined the T_A threshold (π) as a minimum difference, between the new T_L and the T_L in the last recommendation sent, above

which nodes must announce the new T_L by sending a T_A. The reception of a T_A message does not imply a recalculation of the trust level to reduce the effect of malicious nodes that send T_{As} to trigger trust level recalculation in other nodes. The recalculation is triggered by the perception of an action.

3.6 Authentication mechanism

An authentication mechanism is essential, because malicious nodes may pretend to be another node. Nevertheless, our model does not require a sophisticated authentication mechanism. Nodes do not need to know nor recognize any other node *a priori*, namely, a node does not need to identify a new neighbor when it arrives. In our system, nodes must be able to identify neighbors that they already know. Therefore, there is no need of a certification authority. Hence, nodes must exchange identifiers when they first meet and keep a neighbor identifier during all the period they remain in the radio range of each other. Thus, a pair of public/private key for each node is enough to allow our mechanism to work adequately. It is important to notice that there is no correct identifier and a node might use different identifiers. However, the Sybil attack is not a real problem for the proposed mechanism, because nodes must behave in order to have a high trust level. Therefore, even though a node may have multiple identities, its neighbors will be able to identify the benign ones, and will avoid interacting with the malicious ones Nevertheless, authentication mechanisms are not in the scope of this work.

3.7 THE TRUST MODEL IMPLEMENTATION

Home made simulator has been developed, which is specifically designed for this model, in order to evaluate and identify the main characteristics of the proposed model. In ad hoc networks, nodes can perform several actions, like sending packets, forwarding packets, responding to routing messages, sending recommendations, among others. The set of performed actions define the node's behavior. Therefore, the Learning plan monitors the neighbor's actions trying to evaluate their behavior. In our simulator, each node performs good actions and/or bad actions. The time between two consecutive actions performed by a node is exponentially distributed (mean = 5 time units). The kind of action that will be performed depends solely on the nature of the node. A node with a nature equals to 0.8 means that it performs eight good actions out of ten. The nature of a node ranges from 0 to 1. Trustworthy nodes have nature equals to 1 while untrustworthy nodes have nature equals to 0. The nature is used as a reference of the ideal global trust level that a node should receive by its neighbors. We use it here as a metric to evaluate how close the measured global trust level of a node actually gets from its nature. We emulate the Behavior Monitor (Fig.3.4) by introducing in our simulator the concept of perception. The perception indicates the probability of noticing a certain action. Each Behavior Monitor presents its own perception. Therefore, a node with a perception of 0.6 is able of noticing 60% of all the actions performed by its neighbors. The Behavior Monitor passes all the perceived actions to the Classifier without knowing its nature. In our simulator, we assume a perfect Classifier, which means that the judgment of an action always

matches with the original nature of the action. It is worth to mention that noticing and judging an action does not imply using promiscuous mode. We believe that a node should be able to decide whether it will use promiscuous mode or not based on its own constraints and needs. Thus, nodes may decide not to use promiscuous mode at the expense of having a lower perception. Therefore, the perception parameter can reflect nodes that operate in simple and intermediate modes. Finally, the judgments are transmitted to the Experience Calculator. For the Experience Calculator, we propose a simple approach which consists of evaluating the trust value based on a set of the last i perceived actions from the same neighbor. This implies the existence of a minimum number of actions i_{min} that a node must notice from each neighbor before having a concrete opinion about them, based on its own experience. It means that during the initial phase of first contact, nodes use just the recommendations of its neighbors to evaluate the trust level of the new one. The minimum number of perceived actions is crucial for the accuracy of the measure. A higher perception allows a more accurate result. At the same time, a large number of necessary initial actions leads to a longer delay for assessing the trust value for new neighbors, leading to a higher convergence time. For the simulations, we assume the Experience Calculator considers the last 10 actions from a neighbor to estimate the trust value.

Chapter Four

Simulation and results

Simulation and results

Home made simulator has been developed, which is specifically designed for this model, in order to evaluate and identify the main characteristics of the proposed model.

Software Specification:

Operating System	:	Windows 98/2000/XP
Language	:	C#.NET, including multi-threading and networking **libraries**
Server	:	IIS
Framework	:	V2.0

Hardware Specification:

RAM	:	256 MB and above
Processor	:	P3 and above
Hard Disk	:	40 GB and above

Our concern is different from other works that focus strictly on security issues. We focus on providing nodes a way of having an opinion about their neighbors. This opinion governs the interaction among nodes. The goal is to make nodes capable of making their own decisions based on the autonomic paradigm.

So the main goal here is to evaluate and analyze:

- The influence of the number of neighbors.
- The first trust assignment strategy.
- The variation of parameters *alpha* and *perception*.
- Analyzing the impact of the relationship maturity.

- Evaluating the performance of the CEP protocol.

The simulation scenario consists of 32 nodes with 250 m transmission range, which are randomly placed in a 150 m × 150 m area. Under these circumstances, all nodes can communicate directly to each other, characterizing a single hop ad hoc network.

We chose *alpha* = *beta* = *perception* = 0.5. These are the standard values for the simulations. All nodes have the same nature.

Figure 4.1 presents the time response of the average trust level from all neighbors about a specific node. We observe in Figure 4.1.a that the trust level value begins in a certain level but tends to the expected trust level. The expected (correct) level is the nature of the node that is being analyzed. After a specific amount of time, the curve oscillates around the correct value. Because according to:

$$T_a(b) = (1-\alpha)F_a + \alpha R_a(b), \qquad (6)$$

Initially there is no recommendations, so the trust level begin at Fa,which is in the optimistic strategy equal to 0.9. and after receiving recommendation it tends to the expected trust level which is equal to the nature of of the node = 0.2.

Thus, we verify the existence of a transient period and stationary period. In the transient period Fig. 4.1.a, nodes are trying to approximate to the expected value, while in the stationary period Fig. 4.1.b, the trust level is almost stable, very close to the correct value.

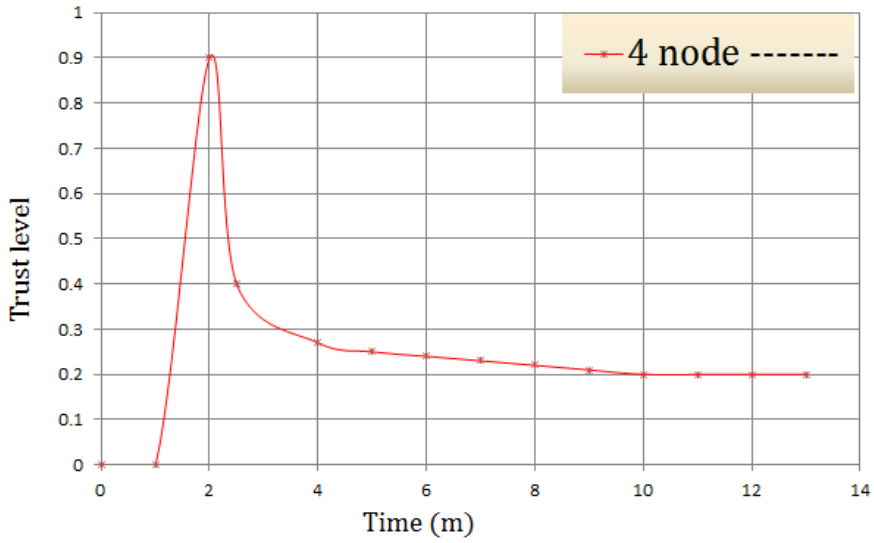


Fig. 4.1.a. The variation of trust level during time, (The transient period).

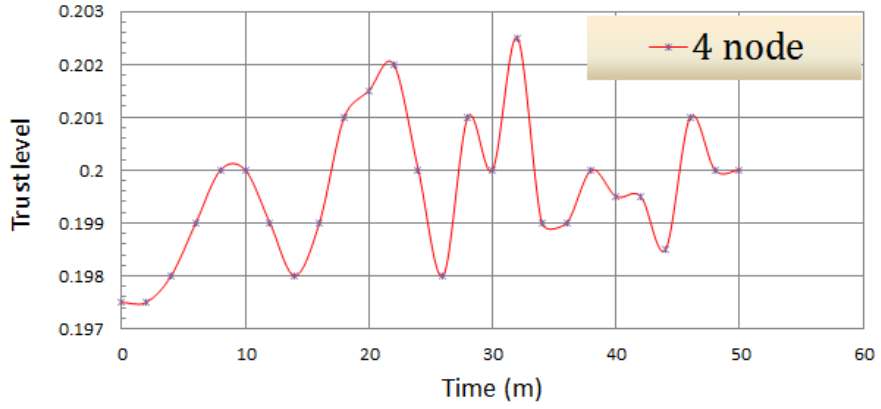


Fig. 4.1.b. The variation of trust level during time. The stationary period.

In the following figures, instead of presenting the average trust level, we present the average error of the trust value evaluated, that is, the difference between the trust level and the correct value. At the end, the ideal result is a curve that reaches the value zero, which means that there is no error between the average trust values calculated by the neighbors and the value of the nature of the node.

In Figure 4.2, nodes adopt an optimistic strategy and we vary the number of neighbors. The nature is set to 0,2. We can notice that the greater is the number of neighbors the closer to zero is the error. It occurs due to the fact that augmenting the number of neighbors means increasing the number of recommendations, which implies a greater probability of receiving recommendations closer to the correct value.

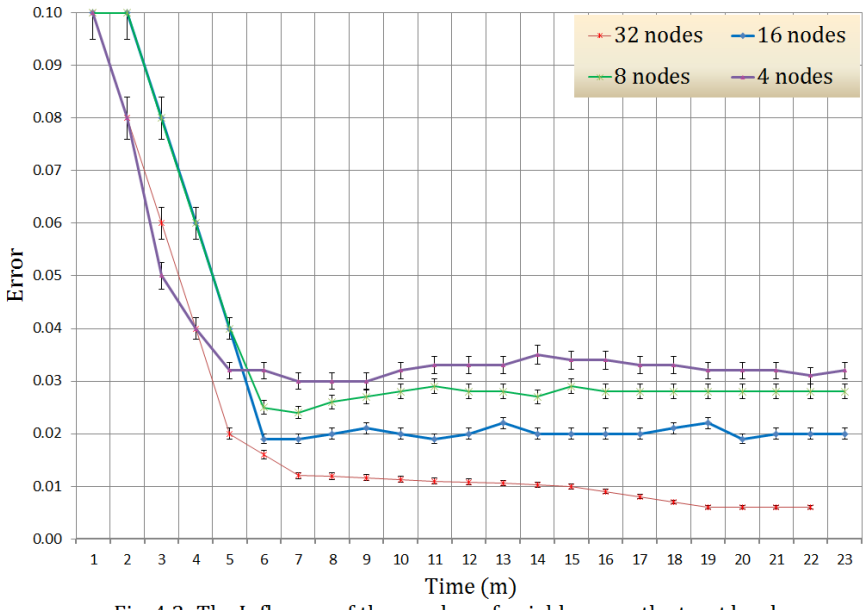


Fig. 4.2. The Influence of the number of neighbors on the trust level error

Figure 4.3, shows the influence of the parameter alpha on the trust level evaluation. According to Eq: $T_a(b)=(1-\alpha)Q_a(b)+\alpha R_a(b)$, (1) Decreasing alpha implies that the recommendation of other nodes has a minor effect in the trust level calculation where reducing the effict of the experience.

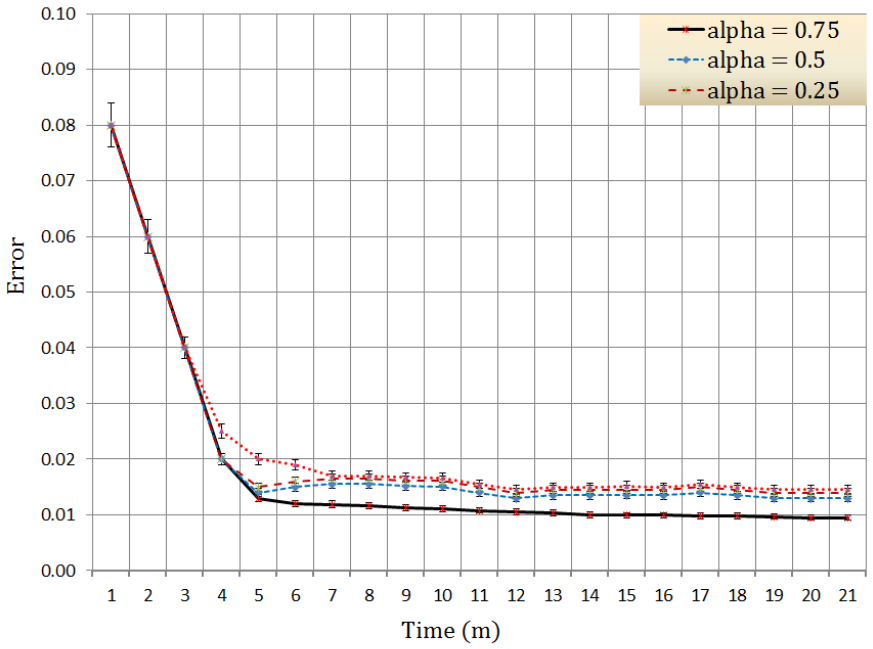


Fig.4.3. The Influence of alpha on the trust level error

Figure 4.4 reveals the effect of the perception on the trust level evaluation. It is clear that the perception is strong related to the duration of the transient period. It occurs due to the existence of a minimum number of actions from each neighbor for nodes to consider its own experiences.

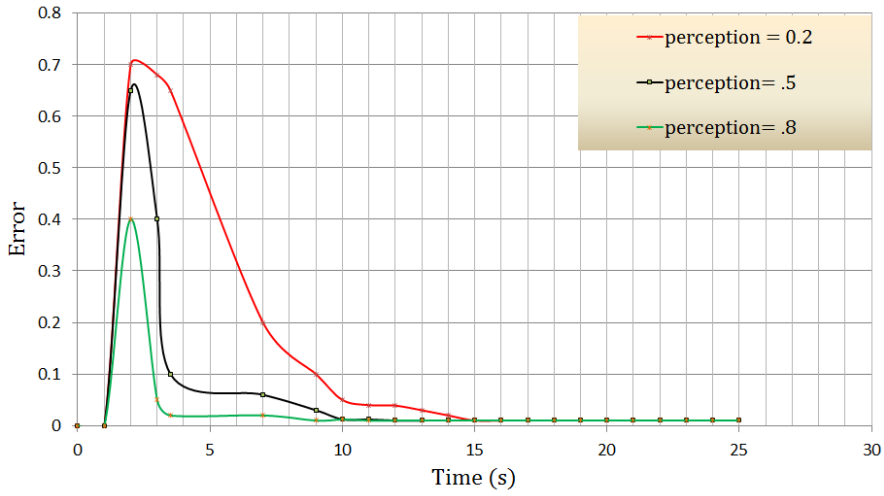


Fig.4.4. The Influence of perception on the trust level error

With low perception the importance of the number of neighbors to reach closer to the expected value is clearer. It means that the lowest is the perception, the lowest is the probability of noticing the real nature of a neighbor by the judgment of its actions. On the other hand, a low perception can be compensated by a larger number of neighbors as shown in figure 4.5.

Figure 4.6 presents the influence of the nature on the trust level evaluation. That the nature does not affect significantly the duration of the transient, only the peak, according to the chosen strategy.

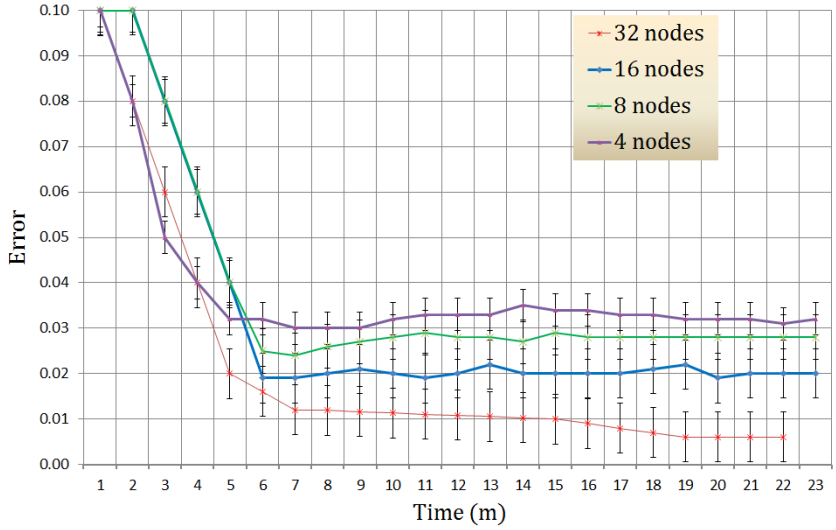


Fig.4.5. The effict of the number of neighbours in case of low perception

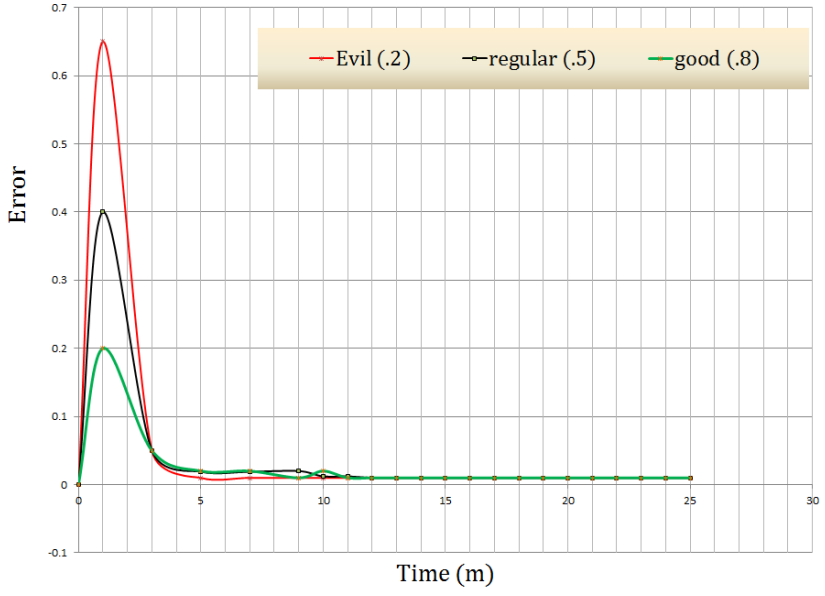


Fig.4.6. The influence of the nature on the trust level error

At last, we analyze the impact of the relationship maturity in the evaluation of the trust level, For this purpose, we present a simple scenario with a specific mobility pattern, which consists of 21 nodes with 250 m transmission range, which are placed in a 1000m × 400m area, as shown in Fig. 4.7. The distance between nodes is 150 m.

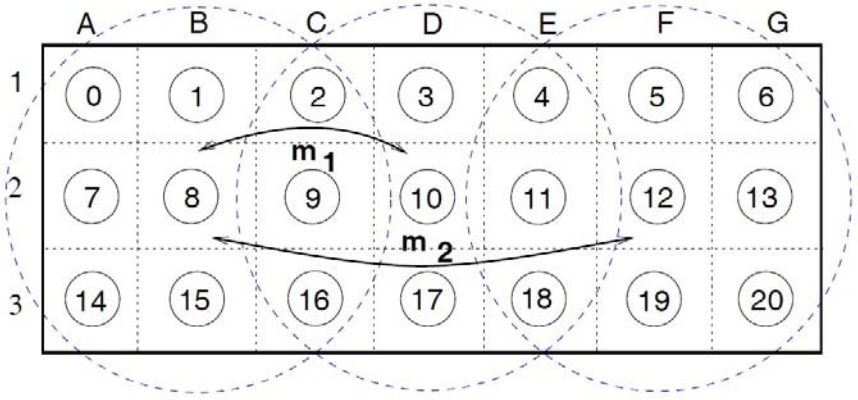


Fig. 4.7. The multihop experiment scenario.

All nodes have the same *nature* equals to 0.2, and we assume the perception is equal to 0.5, and the first trust assignment strategy is optimistic, hence the new node assigned a trust level equal to 0.9. These are the standard values for the simulations which chosed as the worst case parameters.

To measure the impact of the relationship maturity, we assume node 8 going to move to zone F2, the same zone as node 12 (scenario m_2). We consider the trust level evaluation of node 8 by node 6. Therefore, when node 8 arrives at the destination zone F2, it has no old neighbors, node 6 will treat all the recommendations about node 8 as the same (no maturity used). The same scenario happen when node 8 moves to zone D2, the same zone as node 10 (scenario m_1). But if we

consider the trust level evaluation of node 8 by node 4, hence it has 3 old neighbors (node2, node9, node16).

Without the relationship maturity, when node 4 receives the recommendations of its neighbors, it will treat them all the same manner.

Using the relationship maturity, node 4 gives more importance to the recommendations of (node 2, node 9, node 16) which is the oldest neighbors of node 8.

It can be noticed in Fig.4.8 that the transient is shorter with the relationship maturity. We can have almost the same effect of increasing *alpha* just by using the relationship maturity.

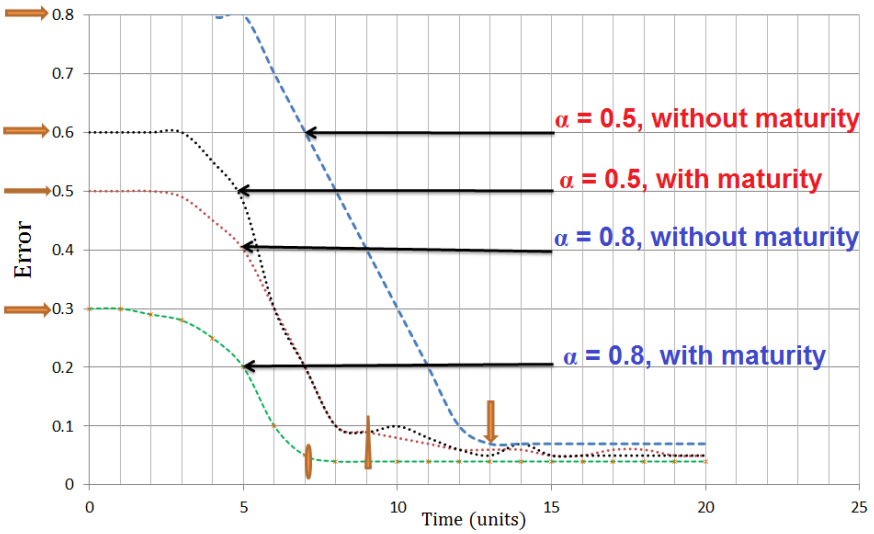


Fig.4.8. The impact of the relationship maturity on the trust level error, varying α .

The figure also shows that with a greater *alpha* the impact of the relationship maturity in the transient is more significant. It improves the efficiency of the system due to the fact that node 4 prioritizes the recommendations of its neighbors. Therefore, giving more weight to the recommendations from nodes that have a longer relationship with the target node is more effective. Although node 8 is not able to reach the stationary period, it achieves a lower Error rate than without using the relationship maturity.

The Contribution Exchange Protocol (CEP) (Section 3.5) is an important feature in this model. In order to evaluate the performance of the CEP protocol a single-hop network is used, because it is a "local" protocol, that is, the interactions are limited to neighbors, and thus mobility does not have a real impact on the performance of CEP. The scenario consists of *n* nodes randomly placed in a 150 *m* $\times$ 150 *m* area, which means that each node has *n*-1 neighbors. The first trust value is 0.9, all nodes have a nature equals 0.2. All nodes arrive at the same time and try to evaluate the trust level of their neighbors.
As we mention in section 3.5, The protocol is composed of three messages:

- Trust Request (T_{REQ}) message.
- Trust Reply (T_{REP}) message.
- Trust Advertisement (T_A) message

We believe that this is a representative scenario, since in this scenario all types of messages are used. The first set of simulations aims at evaluating the impact of the number of neighbors on the performance

of the CEP protocol, more specifically on the number of sent messages. Therefore, we vary the number of nodes n from 4 to 32.

Figure 4.9. presents the result of the number of messages sent per node in this scenario. The T_{REQ} message is sent just once when two nodes first meet. Thus, each node should send at most $n - 1$ T_{REQs}. However, we implement a timer before sending a T_{REQ} message that is used to collect the maximum number of T_{REQs} in one single message. The timer also permits the T_{REQ} suppression when the node receives a T_{REP} during the timer period. This approach allows reducing significantly the number of T_{REQs} when the neighborhood changes in short-term period, as in the case of a network in which nodes start simultaneously. Results show the effectiveness of this approach. In this scenario we reach more than 85% of reduction (the case with 32 nodes).

The T_{REP} message is sent just once per T_{REP} request, which means that the expected number of T_{REPs} $(n - 1)(n - 2)$ messages. First, we implement the TREP as a broadcast message which is only considered by nodes that have sent a T_{REQ} recently. Thus, the number of expected messages drop to $(n - 1)$. Finally, we implement the same timer approach for the T_{REP}. Figure 4.9 shows that for the T_{REP}, these two approaches are can reduce the number of T_{REPs} by more than 99%.

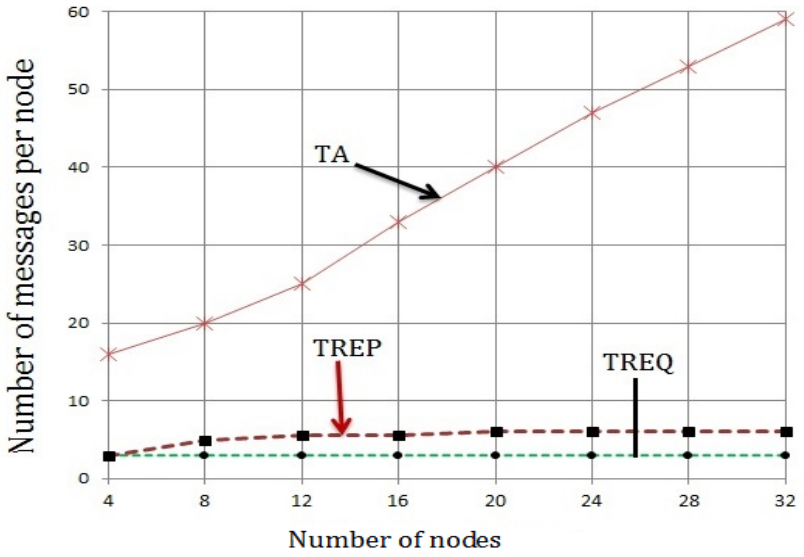


Fig. 4.9. The influence of the number of neighbors on the number of messages.

We notice from the previous result (Fig. 4.9) that the TA message is more sensitive to the increase of the number of neighbors. However, we observe that there is no exponential increase (*mostly* $\frac{3n}{2} \rightarrow O(\mathrm{n})$) and if we consider that these messages are sent at each transient period, we have less than one T_A message per unit of time during the transient period.

We can try to optimize the number of T_A messages sent during the transient period. T_A messages are sent by nodes whenever the trust level of a given neighbor has varied more than a certain threshold (π). This approach avoids sending trust level information after every change in the trust level of a neighbor, instead, we advertise the trust

level information just after a significant change compared to the last advertised value.

In Fig. 4.10, we use the same scenario but with 20 nodes. it shows the impact of the value of π on the number of messages.

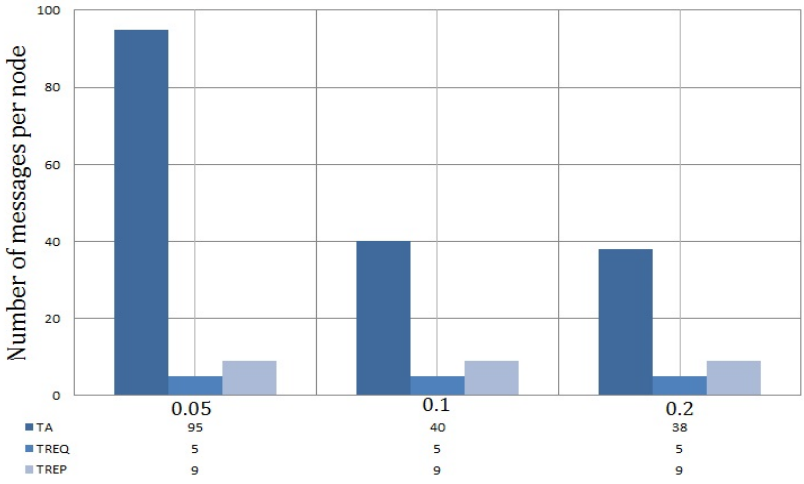


Fig. 4.10. The impact of the trust level variation threshold(π) on the number of messages per node.

The first important observation is that, as expected, T_{REQ} and T_{REP} messages are not influenced by the value of π. Second, the lower is the value of π, the larger is the number of TA messages and the faster is the transient period. An interesting result is that setting π = 0.2 does not reduce significantly the number of messages, comparing to π = 0.1, because the trust level variation is smoother which leads to a longer transient period. Moreover, for π = 0.2 the trust evaluation process does not converge to the correct value (0.2). Therefore, there is an optimum value for π that reduces the number of TA messages and provides a fast and correct convergence.

Chapter Five

Conclusion

Conclusion

A human-based trust assignment model for ad hoc networks have been proposed. It aims at building a trust relationship among nodes inspired by the human concept of trust. Our concern is different from other works that focus strictly on security issues. We focus on providing nodes a way of having an opinion about their neighbors. This opinion governs the interaction among nodes. The goal is to make nodes capable of making their own decisions based on the autonomic paradigm. The proposed model results in a utterly distributed trust system for ad hoc networks based on the recommendation of other nodes and on the own experiences of the nodes. This approach considers not only the trust level but also its accuracy and the relationship maturity. We also define the Contribution Exchange Protocol (CEP) that allows nodes to exchange recommendations in an efficient way. The system performance is analyzed through simulations. The results reveal the Effectiveness of the proposed system and show the influence of the main parameters.

Results shows the Scalability of the proposed model, which is a key problem when we consider a large network size, networks of 10,000 or even 100,000 nodes, due to the limited memory and processing power on mobile devices. The proposed model improves scalability by restricting nodes to keep and exchange trust information solely with direct neighbors.

Future work

Future work includes defining and implementing a monitoring scheme for a specific application and applying our model to improve the service/application performance, as for instance, an authentication protocol.

Another issue that needs more research and implementation effort is the selection of neighbor subset ka, we define it as:

$$Ka = \{ \forall i \in Na \mid Ta(i) \geq Tth \cap Ma(i) \geq Mth \}$$

but node may has an upper trust level, where the maturity factor is low, so we need sophisticated strategy to decide the best neighbor subset ka.

Deciding the best strategy to derive *Fa* is not a simple task. For instance, *Fa* must take into account the level of mobility, the current satisfaction, the number of reliable neighbors. As choosing the best strategy evolves several parameters, we suggest a learning approach to select the strategy. This means that the Learning layer is responsible for selecting the best strategy.

References

[1] C. E. Perkins, Ad Hoc Networking, 1st edition. Addison-Wesley Professional,2001.

[2] D. Artz and Y. Gil, “A survey of trust in computer science and the semantic web," Web Semantics: Science, Services Agents World Wide Web, vol. 5, no. 2, pp. 58-71, June 2007.

[3] A. Josang, “Trust and reputation systems," in Foundations Security Analysis Design IV, FOSAD 2006/2007 - Tutorial Lectures, (Bertinoro, Italy), Springer LNCS 4677, Sep. 2007.

[4] A. Boukerch, L. Xu and K. EL-Khatib, “Trust-based security for wireless ad hoc and sensor networks,” Computer Communications, no. 30, pp. 2413–2427, 2007.

[5] M. A. Ayachi, C. Bidan, T. Abbes and A. Bouhoula, “Misbehavior detection using implicit trust relations in the AODV routing protocol,” in International Symposium on Trusted Computing and Communications, Trustcom, pp. 802–808, 2009.

[6] J. H. Cho, A. Swami and I. R. Chen, “Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks,” in International Symposium on Trusted Computing and Communications, Trustcom, pp. 641–650, 2009.

[7] D. H. Mcknight and N. L. Chervany, “The meanings of trust: University of Minnesota, Technical reports.” http://misrc.umn.edu/wpaper/WorkingPapers/9604.pdf, 1996.

[8] A. Josang. The right type of trust for distributed systems. In NSPW ’96: Proceedings of the 1996 workshop on New security paradigms, pages 119–131, New York, NY, USA, 1996. ACM Press.

[9] D. Harrison McKnight and Norman L. Chervany. Trust and distrust definitions: One bite at a time. In Trust in Cybersocietites, Integrating the Human and Artificial Perspectives, pages 27–54, London, UK, 2000. Springer-Verlag.

[10] D. Gambetta, “Can we trust trust,” Trust: Making and breaking cooperative relations, vol. 13, pp. 213–237, 2000.

[11] R.J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., New York, NY, USA, 2001.

[12] L. Butty´an and J.-P. Hubaux. Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing. Cambridge University Press, 2007.

[13] G. Athanasiou, L. Tassiulas, and G. S. Yovanof. Overcoming misbehaviour in mobile ad hoc networks: An overview. Crossroads The ACM Student Magazine, (114):23–30, 2005.

[14] M. Conti, E. Gregori, and G. Maselli. Cooperation issues in mobile ad hoc networks. In ICDCSW ’04: Proceedings of the 24th International Conference on Distributed Computing Systems Workshops - W7: EC (ICDCSW’04), pages 803–808, Washington, DC, USA, 2004. IEEE Computer Society.

[15] M. Deutch, “Cooperation and trust: Some theoretical notes,” Nebraska Symposium on Motivation, Nebraska University Press, pp. 275–319, 1962.

[16] P. Sztompka, “Trust: A sociological theory,” in Cambridge: Cambridge University Press, 1999.

[17] R. C. Mayer, J. H. Davis and F. D. Schoorman, “An integrative model of organizational trust,” Academy of Management Review, vol. 20, pp. 709–734, 1995.

[18] D. J. McAllister, “Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations,” Academy of Management Journal, no. 38, pp. 24–59, 1995.

[19] D. Olmedilla, O. Rana, B. Matthews, W. Nejdl, “Security and trust issues in semantic grids,” in Proceedings of the Dagsthul Seminar, Semantic Grid: The Convergence of Technologies, vol. 05271, 2005.

[20] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decis. Support Syst., vol. 43, no. 2, pp. 618–644, 2007.

[21] D. Gambetta, "Can we trust trust?," Trust: Making and Breaking Cooperative Relations Gambetta, D (ed.). Basil Blackwell. Oxford, pp. 213–237, 1990.

[22] L. Mui, M. Mohtashemi and A. Halberstadt, "A computational model of trust and reputation," in Proceedings of the 35th Hawaii International Conference on System Science, HICSS'02, 2002.

[23] G. Theodorakopoulos and J. S. Baras, "A testbed for comparing trust computation algorithms." http://infoscience.epfl.ch/record/111326/files/gtjb- asc06a.pdf.

[24] L. Mui, M. Mohtashemi and A. Halberstadt. ''A Computational Model of Trust and Reputation'', Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS 2002). Hawaii, USA, pp. 2431–2439, 2002.

[25] Mobile Ad hoc Networks.
http://en.wikipedia.org/wiki/Mobile ad-hoc network.

[26] J.Jubin and J.D.Tornow. Darpa packet radio network protocol. In Proceedings of the IEEE, volume 75, pages 21–32, Jan 1987.

[27] E. M. Belding-Royer and C. K. Toh. A review of current routing protocols for ad-hoc MANETs. IEEE Personal Communications Magazine, pp. 46–55, 1999.

[28] 2. C. E. Perkins. Ad hoc networking. Addison-Wesley, 2001.

[29] Guide to Wireless Ad Hoc Networks, Sudip Misra, Isaac Woungang,Subhas Chandra, Misra, 2009.

[30] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. Mobile Computing. pp. 153–181, 1996.

[31]. C. E. Perkins and E. M. Royer. Ad hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999.

[32] Lim, H. and Kim, C. (2000). Multicast tree construction and flooding in wireless ad hoc networks. In Proceedings of the 3rd ACM international workshop on modeling, analysis and simulation of wireless and mobile systems, ACM Press, pp 61–68.

[33] Tseng, Y.-C., Ni, S.-Y., and Shih, E.-Y. (2001). Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network. In Proceedings of the International Conference on Distributed Systems, Washington,DC, USA, pp. 481–488.

[34] S. Capkun and J.-P. Hubaux. ‘‘BISS: Building Secure Routing out of an Incomplete Set of Security Associations’’, Proceedings of the 2003 ACM Workshop on Wireless Security, San Diego, CA, USA, pp. 21–29, 2003

[35] Y.-C. Hu and A. Perrig. ‘‘A Survey of Secure Wireless Ad Hoc Routing’’. IEEE Security and Privacy, 2(3), 28–39, 2004.

[36] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang. ‘‘Self-securing Ad Hoc Wireless Networks’’, Proceedings of the IEEE ISCC, 2002.

[37] S. Capkun, L. Buttyan and J.-P. Hubaux. ‘‘Self-Organized Public-Key Management for Mobile Ad Hoc Networks’’, Proceedings of the ACM International Workshop on Wireless Security (WiSe 2002), 2002.

[38] S. Buchegger and J.-Y. L. Boudec. ‘‘A Robust Reputation System for P2P and Mobile Ad-hoc Networks’’, Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems (P2PEcon 2004), Harvard University, Cambridge MA, USA, pp. 2004.

[39] S. Buchegger and J.-Y. L. Boudec. ‘‘Self-Policing Mobile Ad-hoc Networks’’ in Mobile Computing Handbook, M. Ilyas and I. Mahgoub, Ed.: CRC Press, USA, 2004.

[40] A. A. Pirzada, C. McDonald and A. Datta. ‘‘Dependable Dynamic Source Routing without a Trusted Third Party’’, Proceedings of 28th Australasian conference on Computer Science, Newcastle, Australia, pp. 79–85, 2005.

[41] S. Yan Lindsay, Y. Wei, H. Zhu and K. J. R. Liu. ‘‘Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks’’. IEEE Journal on Selected Areas in Communications, 24(2), 305–317, 2006.

[42] V. Balakrishnan, V. Varadharajan, P. Lucs and U. Tupakula. ‘‘Trust Enhanced Secure Mobile Ad hoc Network Routing’’, 2nd IEEE International Symposium on Pervasive Computing and Ad Hoc Communications (PCAC 2007), Proceedings of the 21st IEEE International Conference on Advanced Information Networking and Applications Workshops(AINAW 2007), Niagara Falls, Canada, pp. 27–33, 2007.

[43] V. Balakrishnan, V. Varadharajan, U. Tupakula and P. Lucs. ‘‘Trust and Recommendations in Mobile Ad hoc Networks’’, Proceedings of the 3rd International Conference on Networking and Services (ICNS 2007), Athens, Greece, pp. 64–69, 2007.

[44] S. Ruohomaa and L. Kutvonen. ‘‘Trust Management Survey’’, Proceedings of the 3rd International Conference on Trust Management (iTrust 2005), Rocquencourt, Fran[47] ce, pp. 77–92, 2005.

[45] L. Mui, M. Mohtashemi and A. Halberstadt. ‘‘A Computational Model of Trust and Reputation’’, Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS 2002). Hawaii, USA, pp. 2431–2439, 2002.

[46] S. Buchegger and J.-Y. Le Boudec. Performance analysis of the CONFIDANT protocol: Cooperation of nodes fairness in dynamic ad-hoc networks. Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing, 2002.

[47] S. Buchegger and J. Y. Le Boudec. The effect of rumor spreading in reputation systems for mobile ad-hoc networks. Proceedings of WiOpt `03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2003.

[48] S. Buchegger and J.-Y. Le Boudec. Coping with false accusations in misbehavior reputation systems for mobile ad-hoc network. Technical Report IC/2003/31, EPFL, 2003.

[49] S. Buchegger and J.-Y. Le Boudec.A robust reputation system for p2p and mobile ad-hoc networks. Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems, 2004.

[50] R. Molva and P. Michiardi. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. IFIP-Communicatin and Multimedia Securtiy Conference, 2002.

[51] S. Bansal and M. Baker. Observation-based cooperation enforcement in ad hoc networks. Technical report 072003, Stanford University, 2007.

[52] W. Yu and K. J. R. Liu, “Attack-resistant cooperation stimulation in autonomous ad hoc networks," IEEE J. Sel. Areas Commun., vol. 23, no. 12, pp. 2260-2271, Dec. 2005.

[53] S. Zhong, J. Chen, and Y. R. Yang, “Sprite: a simple, cheat-proof, creditbased system for mobile ad-hoc networks," in IEEE INFOCOM’03, San Francisco, USA, Apr. 2003.

[54] L. Buttyan and J. P. Hubaux, “Enforcing service availability in mobile ad-hoc wans," in IEEE/ACM MobiHoc’00, Aug. 2000.

[55] L. Buttyan and J. P. Hubaux, “Stimulating cooperation in self-organizing mobile ad hoc networks," ACM/Kluwer Mobile Netw. Appl. (MONET), vol. 8, no. 5, pp. 579-592, Oct. 2003.

[56] J. Crowcroft, R. Gibbens, F. Kelly, and S. Östring, “Modelling incentives for collaboration in mobile ad hoc networks," Performance Evaluation, vol. 57, no. 4, pp. 427-439, Aug. 2004.

[57] J. Pan, L. Cai, X. S. Shen, and J. W. Mark, “Identity-based secure collaboration in wireless ad hoc networks," Comput. Netw., vol. 51, no. 3, pp. 853-865, Feb. 2007.

[58] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks," in ACM MobiCom’00, Aug. 2000.

[59] J. N. Al-Karaki and A. E. Kamal, “Stimulating node cooperation in mobile ad hoc networks," Wireless Personal Commun., vol. 44, no. 2, pp. 219-239, Jan. 2008.

[60] A. Adnane, R. T. de Sousa Jr., C. Bidan, and L. Mé, “Autonomic trust reasoning enables misbehavior detection in OLSR," in ACM Symp. Appl. Comput. (SAC’08), Ceará, Brazil, Mar. 2008.

[61] Y. L. Sun, Z. Han, and K. J. R. Liu, “Defense of trust management vulnerabilities in distributed networks," IEEE Commun. Mag., vol. 46, no. 2, pp. 112-119, Feb. 2008.

[62] G. Theodorakopoulos and J. S. Baras, “On trust models and trust evaluation metrics for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 318-328, Feb. 2006.

[63] Y. Sun, Z. Han, W. Yu, and K. J. R. Liu, “A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks,"in IEEE INFOCOM’06, Barcelona, Spain, Apr. 2006.

[64] Q. He, D. Wu, and P. Khosla, “A secure incentive architecture for ad hoc networks," Wireless Commun. Mobile Comput., vol. 6, no. 3, pp. 333- 346, May 2006.

[65] J. Li, R. Li, and J. Kato, “Future trust management framework for mobile ad hoc networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 108-114, Apr. 2008.

[66] S. Buchegger and J.-Y. Le Boudec, “The effect of rumor spreading in reputation systems for mobile ad-hoc networks," in Modeling Optimization Mobile, Ad Hoc Wireless Netw., Sophia-Antipolis, France, Mar. 2003.

[67] S. Chinni, J. Thomas, G. Ghinea, and Z. Shen, “Trust model for

certificate revocation in ad hoc networks," Ad Hoc Netw., vol. 6, no. 3, pp. 441-457, May 2008.

[68] A. A. Pirzada and C. McDonald, “Trust establishment in pure ad-hoc networks," Wireless Personal Commun.: An International J., vol. 37, no. 1-2, pp. 139-168, Apr. 2006.

[69] K. Komathy and P. Narayanasamy, “Trust-based evolutionary game model assisting AODV routing against selfishness," J. Netw. Comput. Appl. (available online), Feb. 2008.

[70] D. Kostoulas, R. Aldunate, F. P. Mora, and S. Lakhera, “A natureinspired decentralized trust model to reduce information unreliability in complex disaster relief operations," Adv. Eng. Informat., vol. 22, no. 1, pp. 45-58, Jan. 2008.

[71] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, “Quantifying trust in mobile ad-hoc networks," in Proc. IEEE International Conf. Integration Knowledge Intensive Multi-Agent Syst., Waltham, USA, Apr. 2005.

[72] J. O. Kephart and D. M. Chess, “The vision of autonomic computing,"IEEE Computer, vol. 36, no. 1, pp. 41-52, Jan. 2003.

[73] Z. Liu, A. W. Joy, and R. A. Thompson, “A dynamic trust model for mobile ad hoc networks,” in IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS’04), (Suzhou, Chine), May 2004.

[74] Z. Yan, P. Zhang, and T. Virtanen, “Trust evaluation based security solution in ad hoc networks,” in Proceedings of the Seventh Nordic Workshop on Secure IT Systems, (NordSec’03), (Gj˜ A¸vik, Norway), Oct. 2003.

[75] H. Deng, W. Li, and D. P. Agrawal, “Routing security in wireless ad hoc networks,” IEEE Communiations Magazine, pp. 70–75, Oct. 2002.

[76] A. A. Pirzada and C. McDonald, “Establishing trust in pure ad-hoc networks,” in Proceedings of 27th Australasian Computer Science Conference (ACSC’04), (Dunedin, New Zealand), Oct. 2004.

[77] M.K. Reiter, S.G. Stubblebine, “Resilient authentication using path independence”, IEEE Transactions on Computers, Volume 47, No. 12, pp. 1351-1362, December 1998.

[78] U. Maurer, “Modeling a public-key infrastructure”, Proceedings of 1996 European Symposium on Research in

Computer Security (ESORICS '96), pp. 325-350, LNCS Vol 1146, Springer-Verlag, 1996.

[79] A. Jsang, "An algebra for assessing trust in certification chains", Proceedings of the Network and Distributed Systems Security Symposium (NDSS '99), 1999.

[80] D.W. Manchala, "Trust metrics, models, and protocols for electronic commerce transactions", Proceedings of the 18th IEEE International Conference on Distributed Computing Systems, pp. 312-321, May 1998.

[81] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina, "The eigentrust algorithm for reputation management in P2P networks", Proceedings of the 12th International World Wide Web Conferences, pp. 640-651, 2003.

[82] P. Dewan, P. Dasgupta, "Trusting routers and relays in ad hoc networks" Proceedings of the International Conference in Parallel Processing Workshops, Kaohsiung, Taiwan, pp. 351-358, 2003.

[83] F. Azzedin, M. Maheswaran, "Evolving and managing trust in grid computing systems", Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE'02), pp. 1424-1429, 2002.

[84] A. Abdul-Rahman, S. Hailes, "A distributed trust model", Proceedings of ACM New Security Paradigms Workshop, pp. 48-60, Langdale, Cumbria, United Kingdom, 1997.

[85] F. Stajano, R. Anderson, "The resurrecting ducking: security issues for ad hoc wireless networks", Proceedings of the 7th International Workshop on Security Protocols, LNCS 1796, Springer-Verlag, 1999.

[86] L. Eschenauer, V.D. Gligor, J. Barras, "On trust establishment in mobile ad hoc networks", Proceedings of the Security Protocols Workshop, pp. 47-66, LNCS 2845, Springer-Verlag, 2002.

[87] T. Repantis, V. Kalogeraki, "Decentralized trust management for ad hoc peer-to-peer networks", Proceedings of the 4th

International Workshop on Middleware for Pervasive and Ad-Hoc Computing (MPAC), 2006.

[88] A. Patwardhan, F. Perich, A. Josh, T. Finn, Y. Yesha, "Querying in packs: trustworthy data management in ad hoc networks", International Journal of Wireless Information Networks, Vol 13, No 4, 2006.

[89] Y.L. Sun, Z. Han, W. Yu, K.J. R. Liu, "A trust evaluation framework in distributed frameworks: vulnerability analysis and defense against attacks", Proceedings of IEEE INFOCOM'06, pp. 23-29, 2006.

[90] J. S. Baras, T. Jiang, "Managing trust in self-organized mobile ad hoc networks", Proceedings of Networks and Distributed System Security Symposium (NDSS'05), San Diego, CA, USA, 2005.

[91] B-J. Chang, S-L. Kuo, Y-H. Liang, D-Y. Wang, "Markov chain-based trust model for analyzing trust value in distributed multicasting mobile ad hoc networks", Proceedings of the IEEE Asia- Pacific Services Computing Conference, pp. 156-161, 2008.

[92] Y.L. Sun, W. Yu, Z. Han, K.J.R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks" IEEE Journal on Selected Areas in Communications, Vol 24, pp. 305-317, 2006.

[93] J. Sen, P. Roychowdhury, I. Sengupta, "A distributed trust establishment scheme for mobile ad hoc networks", Proceedings of the International Conference on Computing: Theory and Applications, pp. 51-58, 2007.

[94] J. Sen, A. Ukil, D. Bera, A. Pal, "A distributed intrusion detection system for wireless ad hoc networks", Proceedings of the 16th IEEE International Conference on Networking (ICON'08), pp. 1-6, 2008.

[95] S. Bucheggar, J.Y. Boudec, "Performance analysis of the CONFIDANT protocol: cooperation of nodes-fairness in dynamic ad hoc networks", Proceedings of the 3rd Symposium on Mobile Ad-Hoc Networking and Computing, pp. 226-236, 2000.

[96] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, “Providing robust and ubiquitous security support for mobile ad-hoc networks”, Proceedings of 9th International Conference on Network Protocols (ICNP ’01), pp. 251-260, 2001.

[97] J. Hubaux, L. Buttyan, S. Capkun, “The quest for security in mobile ad-hoc networks”, Proceedings of the 2nd ACM International Symposium on Mobile Ad-Hoc Networking and Computing (MobiHoc 2001), pp. 146-155, Long Beach, CA, USA, 2001.